Séquence 1: ”Les adresses IPv6”

Bruno Stévant, Jacques Landru, Jean-Pierre Rioual, Véronique Vèque, Pascal Anelli

MOOC

Objectif IPv6 !

vers l'internet nouvelle génération

Document Compagnon

Séquence 1

Les adresses IPv6

Licence Creative Nommons CC BY-SA 4.0 International

Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0)

Avertissement Ce résumé n'indique que certaines des dispositions clé de la licence. Ce n'est pas une licence, il n'a pas de valeur juridique. Vous devez lire attentivement tous les termes et conditions de la licence avant d'utiliser le matériel licencié.

Creative Commons n'est pas un cabinet d'avocat et n'est pas un service de conseil juridique. Distribuer, afficher et faire un lien vers le résumé ou la licence ne constitue pas une relation client-avocat ou tout autre type de relation entre vous et Creative Commons.

Clause C'est un résumé (et non pas un substitut) de la licence.

http://creativecommons.org/licenses/by-sa/4.0/legalcode

Vous êtes autorisé à :

- **Partager** — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats
- **Adapter** — remixer, transformer et créer à partir du matériel
- pour toute utilisation, y compris commerciale.

L'Offrant ne peut retirer les autorisations concédées par la licence tant que vous appliquez les termes de cette licence.

Selon les conditions suivantes :

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Oeuvre originale, vous devez diffuser l'Oeuvre modifiée dans les même conditions, c'est à dire avec **la même licence** avec laquelle l'Oeuvre originale a été diffusée.

No additional restrictions — Vous n'êtes pas autorisé à appliquer des conditions légales ou des **mesures techniques** qui restreindraient légalement autrui à utiliser l'Oeuvre dans les conditions décrites par la licence.

Notes: Vous n'êtes pas dans l'obligation de respecter la licence pour les éléments ou matériel appartenant au domaine public ou dans le cas où l'utilisation que vous souhaitez faire est couverte par une **exception.**

Aucune garantie n'est donnée. Il se peut que la licence ne vous donne pas toutes les permissions nécessaires pour votre utilisation. Par exemple, certains droits comme l**es droits moraux, le droit des données personnelles et le droit à l'image** sont susceptibles de limiter votre utilisation.

Les informations détaillées sont disponibles aux URL suivantes :

- http://creativecommons.org/licenses/by-sa/4.0/deed.fr
- http://fr.wikipedia.org/wiki/Creative_Commons

Les auteurs

Bruno Stévant

Bruno STEVANT est enseignant chercheur à l'IMT Atlantique. Il intervient dans l'enseignement et sur les projets de recherche autour d'IPv6 depuis plus de 10 ans. Il est secrétaire et responsable des activités de formation de l'association G6, association pour la promotion et le déploiement d'IPv6 en France.

Jacques Landru

Enseignant chercheur au CERI - Systèmes Numériques à l'IMT Nord Europe, Jacques est responsable de l'UV de spécialisation ARES (Architecture des RESeaux) à la fois dans le mode traditionnel présentiel que dans sa déclinaison à distance dans le cadre de la filière apprentissage.

Jean-Pierre Rioual

Ingénieur Conseil Réseaux – EURÊKOM. Fort de 30 années d'expérience dans le domaine des réseaux, il intervient auprès des entreprises pour des missions d'expertise sur leurs réseaux de transmission de données (intégration, mesures, optimisation, administration), conçoit et anime des actions de formation "réseaux".

Véronique Vèque

Véronique Vèque est Professeur des Universités à l'Université Paris-Saclay. Elle enseigne les réseaux depuis plus de 20 ans en Master Réseaux et Télécoms. Elle poursuit ses recherches au sein du L2S (Laboratoire des Signaux et Systèmes) où elle est responsable de l'équipe Réseaux, optimisation et codage. Elle est directrice-adjointe de l'école doctorale STIC de l'Université Paris-Saclay.

Pascal Anelli

Pascal ANELLI est enseignant-chercheur à l'Université de la Réunion. Il enseigne les réseaux depuis plus 20 ans. Il est membre du G6 depuis sa création. A ce titre, il est un des contributeurs du livre IPv6. En 1996, il a participé au développement d'une version de la pile IPv6 pour Linux.

Remerciements à :

- Vincent Lerouvillois, pour son travail de relecture attentive ;
- Joël GROUFFAUD (IUT de la Réunion) ;
- Pierre Ugo TOURNOUX (Université de la Réunion) ;
- Bruno Di Gennaro (Association G6) ;
- Bruno Joachim (Association G6) pour sa contribution à l'activité « Contrôler la configuration réseau par DHCPv6 » ;
- Richard Lorion (Université de la Réunion) pour sa contribution à l'activité « Etablir la connectivité IPv6 tunnels pour IPv6 ».

----- oOo -----

Tables des activités

Activité 10 : Notion d'adressage

Le protocole IP (*Internet Protocol*) assure l'acheminement des paquets d'un bout à un autre du réseau selon un principe de transfert en mode message (également couramment appelé en mode paquet). Dans ce mode d'acheminement, chaque unité de données (*paquet* également appelé *datagramme* dans le contexte IP) est autonome et transite à travers le réseau indépendamment des autres paquets, à l'instar d'une lettre dans le réseau de courrier postal (*cf. l'activité "Qu'est ce que l'Internet" de la séquence "Bienvenue"*).

L'adresse IP

L'adressage est une notion fondamentale dans un réseau. Il a pour rôle d'**identifier** et de **localiser** chacun des nœuds constituant le réseau Internet afin d'assurer le support logique à l'acheminement des paquets.

L'analogie du service postal nous permet d'illustrer les fonctions de l'adressage utilisé dans l'Internet :

- **Identification** : Une adresse IP est un nombre. Ce nombre joue un rôle d'identifiant et il a la propriété d'être unique à l'échelle du réseau. L'adresse IP attribuée à chaque nœud du réseau (*boite aux lettres*) **désigne sans ambiguïté le destinataire** afin que le paquet IP (*le courrier*) soit remis à la bonne interface de communication (*boîte aux lettres du destinataire*).
- **Localisation** : La structure de l'adresse IP est constituée de manière à ce que chaque relai, tels que les routeurs du réseau (*bureaux de poste ou centres de tri*) soit en mesure de **déterminer la route** pour acheminer le paquet **vers sa destination finale**. Le principe de fonctionnement de l'acheminement des paquets sera présenté dans la séquence suivante.

L'adresse IP est codée sur un nombre fixe de bits. Son format est standard ; il est accepté et reconnu par l'ensemble des protagonistes intervenant lors de la communication : émetteur, relais intermédiaires d'acheminement, destinataire (*le cadre destinataire d'une enveloppe doit respecter un ensemble de normes établies : nom, numéro de rue, nom de rue, code postal, ville...*).

Structuration de l'adresse IP

La structure d'une adresses IP comprend deux parties : un préfixe et un identificateur local comme le schématise la figure 1.

- **Préfixe ou localisateur** : Le préfixe identifie le réseau de destination et le localise dans l'infrastructure. Un paquet IP est acheminé à travers le réseau sur la base de ce préfixe.
- **Identificateur local** : Une fois le paquet arrivé dans le réseau de destination, il doit être remis au destinataire final. La partie identificateur local de l'adresse entre alors en jeu.

Figure 1 : Le format d'une adresse IP.

En reprenant l'analogie postale, la lettre est acheminée depuis son point de départ par le bas de l'adresse postale de destination écrite sur l'enveloppe. En tout premier, c'est donc le pays de destination. Puis, au fur et à mesure de son acheminement, la partie significative de l'adresse utilisée remonte. Le code pays est ensuite augmenté du code postal de la ville de destination puis du quartier, de la résidence ou de la rue. À l'arrivée, c'est l'identifiant local, le nom ou le numéro (qui est la partie haute de l'adresse) qui servira au facteur à remettre la lettre dans la boîte du destinataire final. Dans le cas de l'Internet, le principe de l'utilisation de l'adresse est assez proche de cette analogie postale.

Hiérarchisation de l'adressage

L'infrastructure globale des grands réseaux en général, et de l'Internet en particulier, est organisée hiérarchiquement en plusieurs niveaux. En périphérie se trouvent les réseaux "terminaux", connectant les équipements personnels d'un réseau domestique ou l'ensemble des équipements d'une structure ou d'une entreprise. Ces réseaux périphériques sont connectés à un premier niveau d'opérateurs de services réseaux, appelés FAI (Fournisseurs d'Accès à Internet), qui prendra en charge l'acheminement des paquets de et vers l'Internet en les relayant vers le (ou les) niveau(x) supérieur(s). Le niveau supérieur le plus élevé de cette architecture constitue le cœur de l'Internet, couramment dénommé sous le terme anglais *backbone* qui signifie épine dorsale. Il assure l'acheminement entre les grandes régions de l'Internet. Les relais de ces opérateurs de différents niveaux (routeurs IP) assurent la sélection du prochain relai d'acheminement vers la destination.

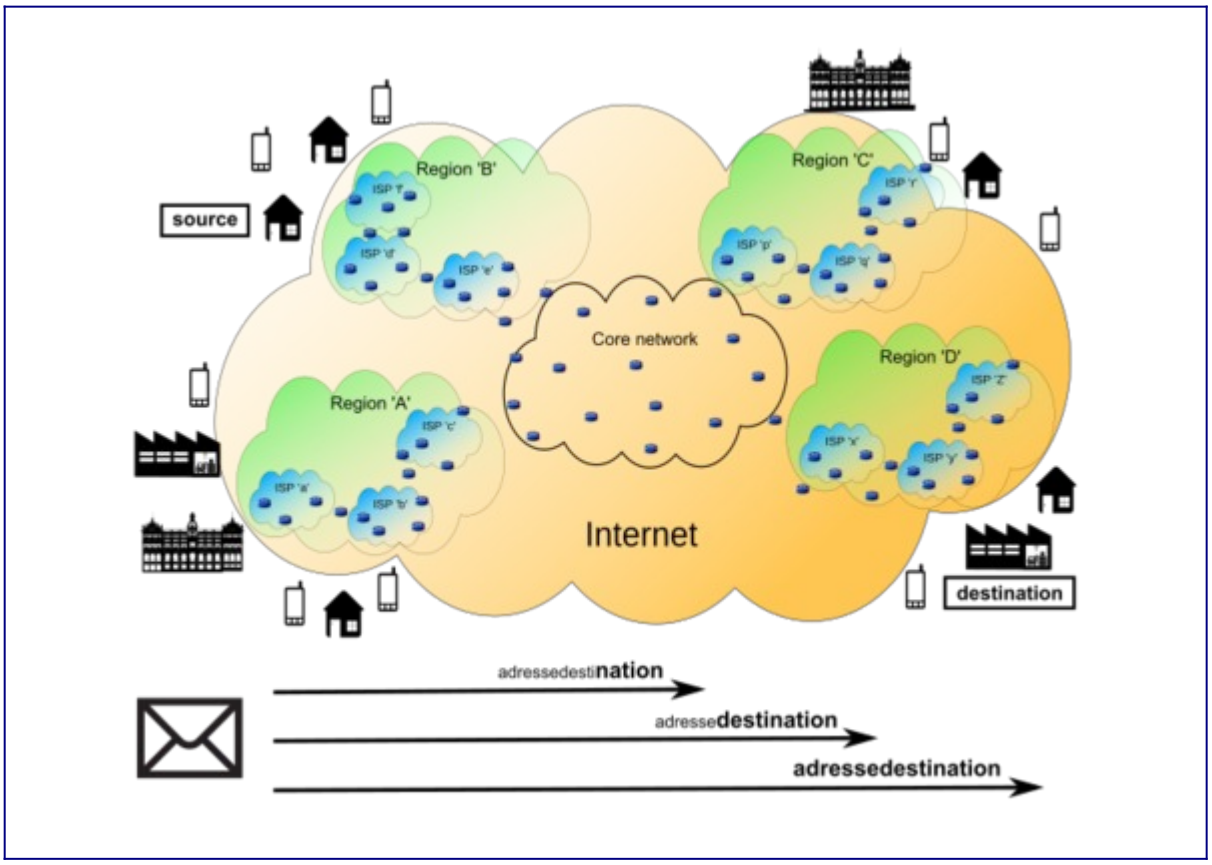

Figure 2 : Partie significative de l'adresse au cours de l'acheminement.

Cette hiérarchisation organisationnelle de l'infrastructure se traduit dans la structuration des adresses. Ainsi, dans le cœur du réseau, les relais des opérateurs en charge de l'infrastructure du *backbone* de l'Internet prennent leur décision d'aiguillage sur la partie de l'adresse identifiant les grandes régions du réseau (*à l'instar de l'aérospostale qui ne s'intéresse qu'au code international de l'adresse pour acheminer les lettres entre les différents continents*). Les opérateurs intermédiaires ont quant à eux besoin d'agréger des informations plus précises de localisation (*le code pays est complété par le code postal de ville ou de métropole urbaine de destination*) pour assurer leur part d'acheminement. Le distributeur local (*bureau de poste*) agrégera la totalité des informations d'adresse pour déposer le paquet à la bonne interface de destination (*le facteur de quartier quant à lui se conformera à la totalité des indications de l'adresse pour distribuer le courrier dans la boite du destinataire*).

Ces informations de localisation du réseau de destination du paquet, prises en compte par les relais des différents niveaux d'acheminement, constituent le préfixe de l'adresse. Le préfixe d'une adresse de destination identifie le réseau vers lequel on doit acheminer le paquet. Le préfixe est donc un identificateur de réseau. La longueur du préfixe utile s'allonge au fur et à mesure que les informations de localisation s'agrègent dans les différents niveaux de l'infrastructure pour préciser la destination. Ainsi, selon sa position dans la hiérarchie, un relai appuie sa décision de sélection du prochain relai sur un préfixe court dans le cœur du réseau et un préfixe de plus en plus long au fur et à mesure que le paquet approche du réseau périphérique de destination (cf. figure 2).

Deux caractéristiques essentielles découlent de cette structuration hiérarchique :

- **Distribution :** Les adresses peuvent être allouées de manière distribuée tout en préservant leur unicité d'identification. L'adresse IP allouée à l'interface d'un équipement est unique et identifie sans ambiguïté cette interface parmi toutes les interfaces connectées au réseau, quelque soit la taille de celui-ci (sur Internet l'ordre de grandeur du nombre d'équipements connectés est de plusieurs milliards). De même, dans le système postal, *Jean Dupont, résidant Place de la République à Lille* n'a pas la même adresse personnelle que *Jean Dupont habitant rue Nationale à Lille*. De plus, ce dernier conservera une boîte aux lettres clairement identifiée lorsqu'il déménagera *rue du Dodo Rieur à Saint-Denis de la Réunion*. L'unicité de l'adresse garantit l'identification sans ambiguïté de la boîte aux lettres de *Jean Dupont* ;
- **Agrégation :** Comme nous l'avons vu ci-dessus, les informations utiles au choix du prochain relai vers le destinataire lors de l'acheminement du paquet agrègent successivement différentes informations dont la précision augmente au fur et à mesure que le paquet approche du réseau destinataire. L'agrégation des préfixes d'adresse contribue à l'efficacité des mécanismes de routage. Dans le cœur de l'Internet, les routeurs prennent leur décisions de routage uniquement sur des préfixes agrégés (les préfixes courts) selon les grandes directions, les routeurs intermédiaires sur des préfixes plus longs, et enfin les routeurs de périphérie sur la totalité du préfixe. Cette agrégation des préfixes permet de réduire le nombre d'entrées dans les tables de routage, ce qui améliore l'efficacité de la fonction de routage. Ainsi, les routeurs de cœur n'ont pas à connaître exhaustivement les routes vers la totalité des destinations possibles, mais

uniquement les routes vers les grandes zones de l'Internet (cf. *analogie de l'aéropostale qui achemine uniquement en se référant au code pays de destination*).

Allocation des adresses IP

Les adresses IP sont allouées aux interfaces des équipements par l'administrateur du réseau auquel l'interface est attachée. Compte tenu des fonctions d'identification et de localisation de l'adresse présentées ci dessus, cette allocation ne peut être quelconque ou aléatoire mais doit se conformer au plan d'adressage défini par l'administrateur du réseau. Le plan d'adressage fixe les identifiants des différents niveaux de la hiérarchie des préfixes relevant du périmètre de responsabilité de l'administrateur. Ces identifiants doivent correspondre aux choix d'organisation de la topologie de l'infrastructure déployée par l'administrateur. En effet, comme on l'a vu, les préfixes sont déterminants dans la localisation du réseau lors de l'acheminement. Ils sont donc une traduction logique de la structuration topologique du réseau. Seule la partie "identificateur local" peut éventuellement être fixée de manière quelconque. (*De la même manière que lorsqu'on emménage dans son logement, une partie de l'adresse postale est fixée par la localisation de l'habitation et le reste est fixé localement par l'habitant lui-même, tel que son nom patronymique ou le nom de villa choisi par le propriétaire.*).

Portée d'une adresse IP

Selon le type de l'adresse, la portée de distribution peut être globale ou limitée :

- **Une adresse de type global** permet d'envoyer un paquet à n'importe quel destinataire du réseau mondial Internet sans restriction (*l'adresse globale peut être utilisée pour envoyer un courrier à une administration, tout aussi bien qu'à son voisin de palier ou à un ami expatrié aux antipodes*).
- **Une adresse de type local** ne permettra quant à elle d'acheminer les paquets que sur son espace de validité (*l'adresse locale de distribution de l'invitation personnelle à la soirée karaoké d'un centre de vacances ou l'adresse locale de distribution de la navette de courrier interne d'un campus universitaire n'est valide que dans son périmètre local, à savoir respectivement, le centre de vacances et le campus universitaire*). En dehors de leur périmètre respectif ces adresses de type local ne sont pas reconnues et ne permettent pas l'acheminement des paquets. Ainsi, l'usage d'adresses de portée locale permet de confiner la distribution des paquets dans un espace exclusivement privatif.

Introduction de la séquence 1

L'adresse IP est l'élément le plus directement et concrètement visible de la nouvelle version du protocole IP pour l'administrateur système et réseaux, chargé de la configuration et de l'administration de l'infrastructure de communication. Avant d'aborder la présentation du protocole et de son fonctionnement, il est important de comprendre les fonctions de l'adresse et de se familiariser avec le formalisme adopté pour sa représentation. C'est l'objectif que nous vous proposons, au travers des différentes activités de cette séquence.

- A11 : la première activité aborde le format d'une adresse IPv6, les fonctions d'une adresse, ainsi que le cycle des différents états d'une adresse lorsqu'elle est allouée à une interface de communication ;
- A12 : l'activité suivante vous permettra de vous familiariser avec le format de notation des adresses IPv6 ;
- A13 : nous enchaînerons avec les différentes déclinaisons des adresses unicast et leurs usages associés ainsi que quelques adresses de multicast nécessaires au fonctionnement d'IPv6 ;
- A14 : cette activité abordera ensuite l'association de ces adresses aux interfaces de communication des équipements par la définition du plan d'adressage du réseau et la politique d'identification des interfaces ;
- Activité pratique : vous pourrez découvrir IPv6 au travers d'une première activité de travaux pratiques. Vous profiterez d’une machine virtuelle intégrant une maquette réseau très réaliste qui vous permettra de tester et observer des communications en IPv6 et de vous familiariser avec différents types d'adresses.

Activité 11 : Fonctions d'une adresse IPv6

Introduction à l'adressage

Le format et la représentation des adresses sont les éléments les plus directement visibles de la nouvelle version du protocole, pour l'utilisateur et l'administrateur réseau. La pénurie des adresses IPv4 étant le premier élément qui a motivé la création d'une nouvelle version du protocole, la définition du nouveau format d'adressage a conditionné certains choix techniques pour IPv6. Bien que les principes de base soient dérivés de ceux employés en IPv4, cet adressage apparaît de prime abord plus complexe. Il est important de se familiariser avec les règles et les principes de représentation et d'attribution avant d'aborder le nouveau protocole.

Fonctions d'une adresse réseau

Dans une architecture IP, une adresse sert à deux fonctions distinctes : l'identification et la localisation

- La fonction d'identification assure qu'une adresse réseau identifie de manière unique une interface ou une machine parmi les "n" machines du réseau. Ce nombre "n" pouvant être arbitrairement grand dans le réseau global Internet par exemple. L'identification permet à deux interlocuteurs de se reconnaître pendant une connexion. Cette vérification est mise en œuvre dans les pseudo en-têtes d'une connexion TCP ou dans les associations de sécurité IPSec par exemple. Il s'agit d'une identification technique de l'interface, restreinte à un contexte de communication. Elle n'est pas permanente et peut varier lorsque l'interface change de liaison. Ainsi, en situation de nomadisme, l'adresse IP varie. Par exemple, lorsqu'un télétravailleur passe de son réseau d'entreprise à un réseau sans fil invité ou au réseau de son domicile, chacun de ces réseaux ayant un préfixe d'identification distinct, l'adresse IP de son ordinateur ou de sa tablette change. Les connexions applicatives qu'il avait établies dans le contexte de son bureau professionnel ne sont plus maintenues et doivent être réinitialisées avec sa nouvelle adresse.
- La localisation est nécessaire à la fonction de routage pour l'acheminement des paquets. L'algorithme du protocole de routage, sur la base de l'information de localisation, assure la remise directe du paquet ou la recherche du prochain relai intermédiaire sur le chemin vers le destinataire. La localisation ne varie qu'en cas de changement de prestataire IP ou de réorganisation du site. Elle est structurée en deux parties : globale et locale.
    - la partie globale de la localisation identifie le réseau parmi les autres réseaux de la topologie. Portée sur la partie haute de l'adresse, elle constitue le préfixe. Elle est significative pour l'acheminement des paquets à travers le réseau. Ainsi, les routeurs du réseau aiguillent les paquets en sélectionnant le prochain routeur relai vers la destination identifiée par le préfixe de l'adresse du destinataire.
    - la partie locale, quant à elle, distingue les interfaces partageant une même liaison ou domaine de diffusion. Elle est portée sur la partie basse de l'adresse. Dans la procédure d'acheminement, elle est significative sur le dernier segment du chemin

pour la remise directe du paquet à l'interface de destination. Ainsi, sur un réseau Ethernet ou un réseau wifi, le nombre d'interfaces partageant le domaine de diffusion est quelconque. Chaque interface se distingue de ses voisines sur la base de cet identifiant local et peut ainsi se reconnaître destinatrice du paquet. La gestion de cette partie locale est assurée par l'administrateur en fonction de sa politique de déploiement des équipements.

Lors des études initiales d'IPv6, il avait été envisagé de séparer les deux fonctions pour faciliter la résolution des problèmes liés à la renumérotation, la mobilité ou la multi-domiciliation. Pour l'instant, la séparation des fonctions est encore à l'état d'expérimentation[1], et les premiers plans d'adressage IPv6 continuent, comme en IPv4, à lier les deux fonctions. De même, comme en IPv4, on considérera qu'une adresse est associée à une interface. Une machine peut posséder plusieurs interfaces. De même, une interface peut supporter plusieurs adresses.

Question de taille

Une adresse IPv6 est un mot de 128 bits (16 octets). Cette taille de 128 bits semble techniquement bien adaptée aux mots manipulés par les processeurs d'aujourd'hui. Les processeurs 32 bits et 64 bits sont aujourd'hui banalisés. Le quadruplement, comparativement à la version précédente d'IP, de la longueur binaire de l'adresse fait apparaître l'adressage IPv6 comme plus "ardu". Cette complexité n'est qu'apparente. Elle traduit la nécessaire adaptation au changement, pour laquelle la plupart d'entre nous montrons naturellement une réticence initiale. Certes, la représentation des adresses de 16 octets a nécessité l'abandon de la notation décimale pointée pour une nouvelle notation hexadécimale (cf. activité suivante), qui est un compromis raisonnable pour la manipulation des adresses par les administrateurs "réseau". Pour la plupart des utilisateurs, l'auto-configuration et la banalisation des services de nommage (DNS - *Domain Name Service*) et des annuaires "réseaux" suppléeront, comme pour IPV4, la nécessité d'avoir à manipuler directement les adresses.

Les principes de structuration de cet adressage dérivent des techniques déjà utilisées en IPv4 ; à savoir une classification de divers plans d'adressage sur les parties hautes de l'adresse (c'est-à-dire sur les préfixes les plus courts) associée à une agrégation des tables de routage, généralisant la méthode dite CIDR - *Classless Inter Domain Routing*. L'usage de divers masques de taille « élastique » permet d'une part, une certaine souplesse dans la définition et l'attribution des préfixes, une optimisation de l'espace d'adressage limitant le gaspillage des larges portions d'adresses, comparativement à IPv4 ; et d'autre part, une optimisation du routage en facilitant sa hiérarchisation : les équipements des opérateurs de cœur de l'internet prennent leur décision de routage sur des préfixes courts, les « grandes directions ». Les équipements de routage des opérateurs de distribution, en périphérie du réseau, routent sur des préfixes plus longs, ce qui a pour effet de maintenir la taille des tables de routage de cœur du réseau dans des proportions raisonnables.

Toutefois, en IPv4, l'amélioration induite par CIDR semble limitée du fait des adresses de 32 bits trop courtes pour permettre une bonne structuration, et du fait qu'il faut assumer le coût du passé : les adresses ont été allouées sans préoccupation d'organisation d'ordre hiérarchique ou

géographique. Malgré ces limitations, l'adressage IPv6 s'appuie *de facto* sur CIDR. La gestion des tables de routage dans le cœur du réseau s'en trouvera quand même améliorée car :

- dès le début, le plan d'adressage est hiérarchisé, éliminant les longs préfixes ;
- les sites multi-domiciliés posséderont autant d'adresses que de fournisseurs de service ;
- des mécanismes de renumérotation automatique faciliteront le changement de préfixes lors du changement de fournisseur d'accès, ou de basculement sur un nouveau plan d'adressage.

Le nombre de combinaisons possibles sur 128 bits (2 à la puissance 128) est "astronomique". Il dépasse les 3,4 x 10 puissance 38 :

- 340 milliards de milliards de milliards de milliards
- Précisément : 340 282 366 920 938 463 463 374 607 431 701 211 156

Certaines estimations encadrent le nombre d'adresses disponibles par mètre carré de surface terrestre, océans compris, entre 1 564 et 3 911 873 538 269 506 102.

1 564 < @ au mètre carré, océans compris < 3 911 873 538 269 506 102

Figure 1 : Estimation de la densité des adresses IPv6 par mètre carré de surface terrestre.

Une citation de Jean Michel Cornu tente de nous en donner une représentation palpable : si on recouvrait la surface de la terre d'une couche de sable de 50 km d'épaisseur (jusqu'en haut de la stratosphère), et que l'on attribue une adresse IPv6 à chaque grain de sable, on n'utiliserait qu'environ deux cent milliardièmes des adresses disponibles. [2]

Sans tomber dans l'optimisme béat de ces grandeurs, ni le pessimisme primitif rappelant qu'au début d'Arpanet (réseau ancêtre d'internet dans les années 1960) les 4 milliards d'adresses possibles d'IPv4 (2 puissance 32) paraissaient également une limite matériellement inaccessible, force est de constater que l'adressage IPv6 est largement dimensionné et qu'une organisation raisonnée de cet espace devrait lui offrir une certaine pérennité. Il est toutefois difficile de prévoir l'utilisation des adresses dans le futur. Ainsi, par exemple, le plan d'adressage actuellement mis en œuvre utilise un identifiant d'équipement de 64 bits, c'est-à-dire la moitié de la taille de l'adresse. En fait, ce genre de calcul n'est qu'un argument pour justifier l'usage de

préfixes d'adresses de taille fixe, qui simplifie le traitement de l'en-tête des datagrammes.

Allocation d'adresses

Un équipement peut posséder plusieurs interfaces de communication. Ainsi, un routeur dispose d'interfaces multiples le connectant à plusieurs réseaux sur lesquels il aiguillera les paquets. De même, nos équipements numériques du quotidien disposent de manière banalisée de diverses interfaces de communication telles que wifi, 5G, bluetooth, USB, ou Ethernet. De plus, **en IPv6, il est important de noter que chacune de ces interfaces supporte généralement plusieurs adresses distinctes simultanément**.

L'allocation des adresses IPv6 à ces interfaces est assurée à la configuration de l'équipement par l'administrateur du réseau, soit manuellement, soit automatiquement. Un ensemble de fonctions de gestion regroupées sous le terme générique anglo-saxon IPAM, signifiant *IP Address Management*, facilite la cohérence de ces allocations. Des mécanismes d'auto-configuration des interfaces peuvent également automatiser l'allocation dynamique des adresses. Ils seront présentés dans une prochaine séquence consacrée à la mise en opération d'un réseau IPv6.

Durée de vie d'une adresse

IPv6 généralisant le plan d'adressage CIDR, les préfixes restent dans tous les cas la propriété des opérateurs. Il ne peuvent plus être attribués "à vie" aux équipements. Les adresses IPv6 sont donc "prêtées" aux interfaces des équipements. L'attribution d'une adresse à une interface est faite temporairement. La durée du prêt (quelquefois appelée durée de vie : *lifetime*) associée à l'adresse indique la durée pendant laquelle l'interface est dépositaire de l'adresse. Quand la durée de vie est épuisée, l'adresse devient invalide. Elle est supprimée de l'interface et devient potentiellement assignable à une autre interface. Une adresse invalide ne doit jamais être utilisée comme adresse dans des communications. La valeur par défaut de la durée de vie d'une adresse est de 30 jours mais cette durée peut être prolongée voire portée à l'infinie (valeur réservée avec tous les bits à 1). L'adresse "lien-local" a une durée de vie illimitée.

Ce système de prêt d'adresse vise à faciliter la renumérotation. La renumérotation de l'interface d'un équipement consiste à passer d'une adresse à une autre. Lors de cette opération, il n'est pas souhaitable de changer brusquement d'adresse. Sinon, toutes les connexions TCP en cours, qui utilisent l'adresse comme identificateur de connexion, seraient brutalement coupées. Ceci pourrait entraîner des perturbations importantes au niveau des applications utilisant TCP à ce moment-là.

Pour faciliter cette transition, un mécanisme d'obsolescence est mis en place pour invalider progressivement une adresse. Ce mécanisme s'appuie sur la capacité d'affectation de plusieurs adresses valides à une même interface. Pour effectuer le choix de l'adresse à utiliser, un état est associé à chaque adresse. Cet état indique dans quelle phase de sa durée de vie une adresse se situe vis-à-vis de l'interface. La figure 2 représente les différents états que prend une adresse depuis sa création. En voici la description.

- Le premier de ces états est qualifié de provisoire (*tentative*). L'adresse a été créée par l'auto-configuration mais son unicité sur le lien n'a pas encore été réalisée. Tant que l'adresse est dans l'état provisoire, elle ne peut être utilisée pour communiquer.
- Une fois que l'unicité a été vérifiée par une procédure dédiée, l'adresse devient valide(*valid*). Elle est effectivement allouée à l'interface.
- Après l'allocation de l'adresse à l'interface, le premier des états valides est qualifié de préféré (*preferred*). L'utilisation de l'adresse n'est aucunement restreinte.
- Peu avant son invalidation, l'adresse passe dans un second état valide dit déprécié (*deprecated*). Son utilisation est déconseillée, mais pas interdite. L'adresse ne doit plus être utilisée comme adresse source pour de nouvelles communications (établissement de connexions TCP par exemple). Par contre, elle peut encore servir d'adresse source pour les connexions existantes. Les datagrammes reçus à une adresse dépréciée continuent à être remis normalement. À la durée de validité, il est également associé une durée de son état préféré.
- Quand l'adresse atteint l'état invalide (*invalid*), elle ne doit plus être utilisée du tout. Le délai du prêt est expiré.

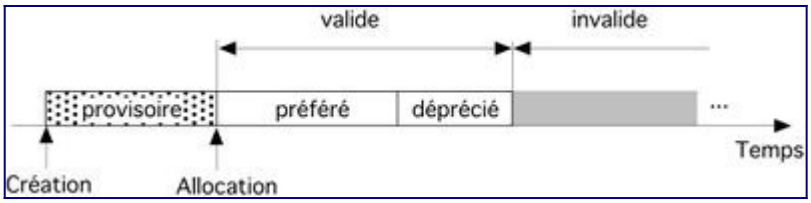

Figure 2 : États successifs d'une adresse sur une interface.

Conclusion

L'adresse est un élément essentiel dans un réseau de communication. Cette activité nous a montré qu'une adresse IP n'est pas qu'un simple paramètre numérique abstrait d'un équipement. L'adresse assure un véritable support fonctionnel d'identification et d'aboutissement des communications. Dans les prochaines activités, nous aborderons le format standard de représentation de l'adresse, reconnu par l'ensemble de l'écosystème IP, ainsi que sa structure distinguant plusieurs catégories d'adresses associées aux différents types de communication.

D'autres aspects vont être développés dans les prochaines activités, notamment :

- la notation des adresses IPv6 ;
- les différents types d'adresses ;
- l'utilisation des adresses.

Références bibliographiques

1. ↕ Bortzmeyer, S. (2009) Création du groupe de travail IETF sur LISP.
2. ↕ Cornu, Jean-Michel (2001) AFING: Fondation Internet Nouvelle Génération

[1]

Pour aller plus loin

Le lecteur intéressé par l'état des travaux sur la séparation des fonctions d'identification et de localisation des adresses pourra consulter les références suivantes :

- Bortzmeyer, S. Séparation de l'identificateur et du localisateur dans Internet
- Meyer, D. (2008). Cisco Internet Protocol Journal, Vol. 11, No. 1.

  The Locator Identifier Separation Protocol (LISP).
- Gurtov, A. and Komu, M. (2009). Internet Protocol Journal, Vol. 12, No. 1. page 27

  Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming.
- RFC 7215 Locator/Identifier Separation Protocol (LISP) Network Element Deployment analyse
- RFC 9063 Host Identity Protocol Architecture analyse

Activité 12 : Notation des adresses IPv6

Introduction

La notation des adresses IPv6 traite du problème de leur représentation textuelle. Il s'agit de définir des règles pour leur affichage, leur manipulation, leur saisie par un utilisateur humain. Le RFC 4291 a posé les principes de la notation d'une adresse IPv6. Le RFC 5952 est venu le compléter pour poser des règles. La notation est importante. Mal maitrisée, elle peut entrainer des problèmes d'interopérabilité comme le montre cet article[1].

Principes

IPv6 a abandonné la notation décimale pointée en usage pour les adresses IPv4 (sur 32 bits, soit 4 octets, on indique la valeur décimale de chaque octet séparée par un point décimal. Exemple : l'adresse IPv4 192.168.0.1). Cette notation est en effet inadaptée pour des chaînes binaires de 16 octets. IPv6 a adopté la notation hexadécimale couramment utilisée dans le monde informatique pour représenter des octets par des couples de chiffres.

Les 16 octets (128 bits) de l'adresse IPv6 suivante se notent en binaire :

00100000 00000001 00001101 10111000 00000000 00000000 00000000 00000000 00001000 00001000 00000000 00100000 00001100 01000001 01111010

et s'écrivent en hexadécimal sous la forme suivante :

20 01 0d b8 00 00 00 00 00 08 08 00 20 0C 41 7A

couramment précédés par le préfixe `0x` pour indiquer que la chaine qui suit est en notation hexadécimale :

0x20010db80000000000080800200C417A

La représentation "textuelle" des adresses IPv6 se fait en segmentant le mot de 128 bits en 8 champs de 16 bits (2 octets) séparés par le caractère ":". Chacun de ces champs est transcrit en 4 chiffres hexadécimaux. L'adresse précédente se note donc :

`2001:0db8:0000:0000:0008:0800:200C:417A`

Par convention, il n'est pas nécessaire d'écrire les zéros de poids fort placés en tête de champ (dans chaque mot de 16 bits, les zéros de poids fort ne sont pas significatifs). L'adresse peut donc prendre une notation plus compacte :

`2001:db8:0:0:8:800:200C:417A`

Plusieurs champs nuls consécutifs peuvent être "abrégés" par l'abréviation " **::** " (2 caractères ':' successifs, sans espace).

`2001:db8::8:800:200C:417A`

Attention : pour éviter toute ambiguïté, cette abréviation ne peut être utilisée qu'une seule fois par adresse !

Exemple	l'adresse	peut également s'écrire
Une adresse unicast	2001:0db8:0:0:0:800:200c:417a	2001:db8::800:200c:417a
Une adresse multicast	ff01:0:0:0:0:0:0:101	ff01::101
Adresse de bouclage (loopback address)	0:0:0:0:0:0:0:1	**::1**
Adresse non spécifiée (unspecified address)	0:0:0:0:0:0:0:0	**::**

Notation canonique pour l'affichage

Les adresses IPv6 peuvent donc avoir plusieurs représentations valides possibles. Le RFC 5952 fournit les recommandations pour une forme de représentation canonique des adresses. Cette forme est destinée aux procédures d'affichage ; par les programmes, les appels systèmes inscrivant des événements dans les fichiers journaux (logs). Cette recommandation ne porte donc que sur les sorties d'adresses (affichage). En entrée (configuration d'équipement, passage de paramètres...), un logiciel devrait toujours accepter les différentes formes valides. La saisie reste donc libre.

Concrètement, selon ce RFC 5952, une adresse devrait être affichée selon la forme suivante :

- Les zéros initiaux (non significatifs) doivent être supprimés.
- L'indication d'une suite de champs nuls consécutifs « :: » doit être utilisée au maximum (sur la série nulle la plus longue). En cas d'égalité, on l'applique sur la première. Exemples :
  - `2001:db8:0:42:0:0:0:1` → `2001:db8:0:42::1`
  - `2001:db8:0:0:42:0:0:1` → `2001:db8::42:0:0:1`
- Les chiffres hexadécimaux doivent être en minuscules.
- Si le numéro de port (TCP ou UDP) doit être indiqué, l'usage de crochets encadrant l'adresse devient obligatoire. Auparavant, cet usage ne l'était que pour les URL. Plus de détails en fin de chapitre.

Notation des préfixes

La notation des préfixes définie par CIDR [RFC 1519] pour IPv4 est conservée pour IPv6. Le préfixe indique le nombre de bits de poids fort de l'adresse (la partie haute de l'adresse ; c'est-à-dire, dans le sens de lecture occidentale, les chiffres à gauche de l'adresse) communs à toutes les adresses appartenant à ce préfixe.

La notation du préfixe d'adresse se fait en séparant l'adresse du nombre de bits du préfixe par un caractère « **/** » (le caractère « diviseur » du pavé numérique de votre clavier).

Adresse-IPv6/longueur-en-bits-du-préfixe

Par exemple, le préfixe suivant :

2001:0db8:0024:a1a0:0000:0000:0000:0000/60

définit 60 bits (affichés ici en caractères gras) qui seront communs à toutes les adresses lui appartenant. Un préfixe peut donc être utilisé pour désigner une plage d'adresses :

Préfixe :	**2001:0db8:0024:a1a**0::/60
Première adresse :	**2001:0db8:0024:a1a**0:0000:0000:0000:0000
Dernière adresse :	**2001:0db8:0024:a1a**f:ffff:ffff:ffff:ffff

Les préfixes permettent donc d'**agréger** en une seule notation plusieurs adresses possédant les mêmes bits de poids forts. Un préfixe permet aussi d'agréger plusieurs préfixes plus spécifiques, c'est-à-dire définissant un nombre plus large de bits communs à un ensemble d'adresses. Ainsi, le préfixe /60 donné dans l'exemple précédent agrège 16 préfixes de largeur 64 bits (/64) :

Le préfixe **2001:0db8:0024:a1a**0::/60 **agrège 16 préfixes /64**

1er préfixe /64 :	**2001:0db8:0024:a1a0**::/64
première adresse :	**2001:0db8:0024:a1a0**:0000:0000:0000:0000
dernière adresse :	**2001:0db8:0024:a1a0**:ffff:ffff:ffff:ffff
2ième préfixe /64 :	**2001:0db8:0024:a1a1**::/64
premère adresse :	**2001:0db8:0024:a1a1**:0000:0000:0000:0000
dernière adresse :	**2001:0db8:0024:a1a1**:ffff:ffff:ffff:ffff
3ième préfixe /64 :	**2001:0db8:0024:a1a2**::/64

première adresse :	**2001:0db8:0024:a1a2**:0000:0000:0000:0000
dernière adresse :	**2001:0db8:0024:a1a2**:ffff:ffff:ffff:ffff
12 préfixes /64 successifs	
.	. .
.	. .
.	. .
16ième préfixe /64 :	**2001:0db8:0024:a1af**::/64
première adresse :	**2001:0db8:0024:a1af**:0000:0000:0000:0000
dernière adresse :	**2001:0db8:0024:a1af**:ffff:ffff:ffff:ffff

Un préfixe peut être utilisé par exemple par la fonction de routage d'un équipement pour désigner la destination d'une route vers un ensemble de machines ou de réseaux (cf. notion de routage du MOOC "Principes des Réseaux de Données").

Cette notation peut être aussi reprise lors de la désignation d'une adresse pour spécifier le réseau auquel elle appartient. Ainsi, dans l'exemple suivant,

le nœud d'adresse	2001:db8:24:a1a1:8:800:200C:417a
appartenant au sous-réseau	2001:db8:24:a1a0::/60
peut se noter	2001:db8:24:a1a1:8:800:200C:417a/60

Cette notation est utilisée notamment lorsque l'on configure une interface réseau avec une adresse, permettant de définir en une seule notation son adresse ainsi que le réseau auquel elle est connectée (qui est représenté par le *netmask* en IPv4).

On notera une petite difficulté dans cette convention de notation pour les préfixes qui ne sont pas alignés sur une frontière de mots de 16 bits, d'octet ou de demi-octet :

l'adresse IPv6	2001:db8:7654:2003::cafe/51
appartient au réseau	2001:db8:7654:2000::/51

La plage d'adresses démarre en	`2001:db8:7654:2000:0000:0000:0000:0000`
et se termine avec	`2001:db8:7654:3fff:ffff:ffff:ffff:ffff`

Notation des URL

Une autre difficulté provient du fait que le caractère "**:**" est significatif dans certains contextes, ce qui peut créer des ambiguïtés. C'est le cas des URL où il est utilisé comme séparateur entre l'adresse et le numéro de port. Les adresses de niveau transport sont des numéros de port TCP ou UDP, cf. MOOC "Principes des Réseaux de Données".

Exemple : l'URL suivante est ambiguë : `http://2001:db8:12::1:8000/` ; en effet, elle peut être interprétée de deux manières :

- le service *web* à l'écoute sur le port http par défaut (le port TCP 80 est le port implicite d'écoute du protocole HTTP) sur la machine d'adresse `2001:db8:12::1:8000`
- les services *web* (protocole HTTP) à l'écoute sur le port TCP 8000 de la machine d'adresse `2001:db8:12::1`

Pour lever cette ambiguïté, le RFC 3986 propose d'inclure l'adresse IPv6 entre "**[ ]**" (crochets ouvrant et fermant). Ainsi, dans le premier cas, l'URL sera notée `http://[2001:db8:12::1:8000]/` et dans le second, `http://[2001:db8:12::1]:8000/`

Les adresses IPv6 unicast embarquant une adresse IPv4

Intégration de l'espace d'adressage IPv4 dans l'espace IPv6

Compte tenu de son étendue, l'espace d'adressage IPv6 peut facilement intégrer l'espace d'adressage IPv4. En conséquence, une adresse IPv4 peut être imbriquée dans une adresse IPv6. Les mécanismes d'interopérabilité IPv6 et IPv4 développés dans la séquence 4 de cette présentation en font usage. Chacun de ces mécanismes d'interopérabilité a fait l'objet d'implémentations diversifiées entraînant des variantes d'imbrication de tout ou partie d'une adresse IPv4 dans une adresse IPv6. Ces variantes seront présentées en détail dans les activités de la séquence 4.

Notation d'une adresse IPv4 dans une adresse IPv6

L'adresse IPv4 est notée sous forme hexadécimale en deux mots de 16 bits séparés par le caractère "**:**". Ainsi, l'adresse IPv4 **`192.168.10.5`** sera notée **`c0a8:a05`** dans l'adresse IPv6.

Exemples :

- `2002:`**`c0a8:a05`**`:624:5054:1ff1fe12:3456`
- `2001:db8:900d:cafe::`**`c0a8:a05`**

Lorsque l'adresse IPv4 occupe la partie basse de l'adresse IPv6 (les 32 bits de poids faible - bits 96 à 127), la notation décimale pointée traditionnelle d'IPv4 est tolérée comme l'indique le RFC 4291. Autrement dit, la notation décimale n'est valide qu'à la fin de l'adresse IPv6. Ainsi, l'adresse `2001:db8:900d:cafe::c0a8:a05` peut être notée `2001:db8:900d:cafe::192.168.10.5` lors d'une saisie (configuration manuelle d'interface ou passage de paramètre en ligne de commande...). Cependant, elle sera affichée sous sa forme canonique (RFC 5952) `2001:db8:900d:cafe::c0a8:a05` dans le journal de bord (log système) de la machine. Dans ce cas, si la saisie peut nous sembler familière, la correspondance entre l'adresse IPv6 et l'adresse IPv4 embarquée est moins évidente à l'affichage.

Conclusion

Nous venons d'introduire la notation des adresses IPv6. Sa maîtrise est importante. Sinon, cela peut entraîner des problèmes d'interopérabilité. Dans les activités suivantes, nous allons approfondir les règles de notations, leurs affectations, et le rôle des différents types d'adresses.

Références bibliographiques

1. ↑ Huston, G. (2013) The ISP Column. March. Literally IPv6

Pour aller plus loin

RFC et leur analyse par S. Bortzmeyer :

- RFC 1519 Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy Analyse
- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax Analyse
- RFC 4291 IP Version 6 Addressing Architecture Analyse
- RFC 5952 A Recommendation for IPv6 Address Text Representation Analyse

Annexe : Vadémécum de notation hexadécimale

Cet aide mémoire, librement inspiré de l'article "Système hexadécimal" de Wikipedia, est destiné à l'accompagnement des auditeurs qui ne sont pas familiers avec cette notation concise des nombres binaires.

Le système hexadécimal est un système de numération en base 16. Il utilise ainsi 16 symboles, en général les chiffres arabes pour les dix premiers chiffres et les lettres **"a"** à **"f"** pour les six suivants (en majuscules ou en minuscules, sans importance en principe, mais il vaut mieux par cohérence adopter l'un ou l'autre pour la notation). Ce système est couramment utilisé en informatique et en électronique numérique pour représenter des codes binaires utilisés par les ordinateurs car il est :

- commode : conversion facile binaire <=> hexadécimal du fait que 16 (nombre de chiffres dans la base hexadécimale) est lui-même une puissance de 2 (nombre de chiffres de la base binaire) ;
- facilement lisible par les opérateurs humains car compact (il réduit le nombre de signes d'un facteur 4 par rapport au binaire). L'unité d'information couramment utilisée en informatique, à savoir l'octet (8 bits), se note ainsi sous forme de 2 chiffres hexadécimaux.

La conversion de binaire en hexadécimal se fait en regroupant les chiffres binaires (les bits) par groupes de quatre, également appelés "quartets" (ou nibbles). Le mot binaire doit donc avoir une longueur multiple de quatre. Au besoin, on le complète par des zéros à gauche (0 de poids fort non significatifs). À chacune des 16 combinaisons binaires d'un quartet (2 puissance 4 = 16) correspond un chiffre hexadécimal.

binaire	Hexadécimal	décimal
0 0 0 0	**0**	0
0 0 0 1	**1**	1
0 0 1 0	**2**	2
0 0 1 1	**3**	3
0 1 0 0	**4**	4
0 1 0 1	**5**	5
0 1 1 0	**6**	6
0 1 1 1	**7**	7
1 0 0 0	**8**	8
1 0 0 1	**9**	9
1 0 1 0	**a**	10
1 0 1 1	**b**	11
1 1 0 0	**c**	12
1 1 0 1	**d**	13
1 1 1 0	**e**	14
1 1 1 1	**f**	15

Conversion

Ainsi, le nombre binaire 0010101011010101 composé de 4 quartets (nibbles) 0010 1010 1101 0101 se note 2ad5 en hexadécimal (0010 => **2**, 1010 => **a**, 1101 => **d**, 0101 => **5**).

Inversement, le nombre hexadécimal 7c8f20 se traduit par la chaîne binaire 0111 1100 1000

1111 0010 0000 (**7** => 0111, **c** => 1100, **8** => 1000, **f** => 1111, **2** => 0010, **0** => 0000) et correspond au code binaire 011111001000111100100000.

Notation

Des notations sont utilisées, notamment dans les langages informatiques, pour différencier sans ambiguïté les chiffres hexadécimaux des autres :

- notation préfixée : 0x123 (langage C et dérivés), &h123 (BASIC), $123 (en Pascal et dérivés comme le VHDL en électronique), mais aussi #123 (Common Lisp), 0h123 (Texas Instruments) ou X'123' (COBOL) ;
- notation suffixée : 123h, 123**(16)** (arithmétique)

(Nota : pour l'anecdote, le chanteur et humoriste Boby Lapointe a inventé en 1968 un système de représentation hexadécimale, appelé système bibi-binaire à la fois drôle et cohérent, basé sur des symboles graphiques convenus en lieu et place des chiffres arabes et lettres (de 'a' à 'f').

Pour aller plus loin

- Le système hexadécimal https://fr.wikipedia.org/wiki/Syst%C3%A8me_hexad%C3%A9cimal
- Le système bibi-binaire https://fr.wikipedia.org/wiki/Syst%C3%A8me_Bibi-binaire
- Nibble https://fr.wikipedia.org/wiki/Nibble
- Une autre forme, moins courante, de représentation des codes binaires : le système octal http://fr.wikipedia.org/wiki/Syst%C3%A8me_octal

Activité 13 : Familles d'adresses IPv6

Introduction

Dans cette troisième activité, nous allons approfondir le rôle des différents types d'adresses IPv6. Après les avoir identifiées, nous découvrirons leurs allocations puis la structure détaillée des préfixes réseau et sous-réseau. Enfin, nous illustrerons la portée des échanges avec ces différentes adresses à travers quelques exemples.

Types d'adresses

IPv6 définit trois types d'adresses : unicast, multicast, anycast.

Terminologie

Un équipement connecté au réseau est dénommé nœud. Si ce nœud est un équipement terminal, on parle d'hôte. Le sous-réseau qui correspond à un réseau local sous-jacent se qualifie, en IPv6, de lien. Tous les nœuds attachés au même lien sont des voisins.

- Le type **unicast** est le plus simple et désigne une interface unique. Une communication unicast signifie que le paquet sera remis à une seule interface identifiée de manière unique par son adresse. La figure 1 montre une communication avec une adresse unicast. La paquet est remis à un seul nœud de destination. Une adresse unicast peut également indiquer une portée qui peut être :
  - globale : unicité de l'identifiant sur l'ensemble de l'Internet (Global Unicast) ;
  - localement restreinte : unicité de l'identifiant étendue à un espace privatif limité à un site ou un campus (Local Unicast) ;
  - restreinte à un lien ou domaine de diffusion de type VLAN (Link-Local Unicast). Une adresse de portée locale (site ou lien) ne sera pas routée (c'est-à-dire transmise) sur l'Internet.

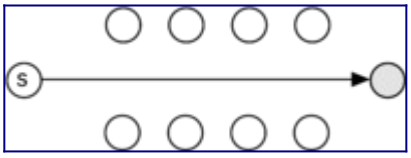

Figure 1 : L'adressage unicast (communication de type 1 vers 1).

- Une adresse de type **multicast** désigne un groupe d'interfaces appartenant à différents nœuds pouvant être situés n'importe où sur le réseau. Lorsqu'un paquet a pour adresse de destination une adresse de multicast, il est acheminé par le réseau à toutes les interfaces appartenant au groupe. IPv6 ne dispose pas d'adresse spécifique de diffusion générale (*broadcast*) au sens reconnu par IPv4, où le paquet est reçu par toutes les interfaces du réseau ou du sous-réseau et non pas toutes les interfaces de l'interconnexion. Le *broadcast* IPv4 est toujours restreint (confiné) à un réseau ou sous-réseau. En IPv4, le *broadcast* est "général" et toutes les interfaces sont à l'écoute. En IPv6, la multi-diffusion est beaucoup plus sélective. On peut s'adresser uniquement aux

routeurs ou aux serveurs DHCP, par exemple. Au niveau lien, un groupe IPv6 permet de s'adresser à l'ensemble des interfaces, offrant par là la même fonction que le *broadcast* restreint d'IPv4. La figure 2 montre une communication utilisant une adresse multicast. Tous les membres du groupe reçoivent le paquet émis par la source.

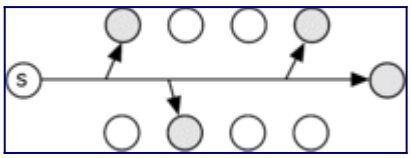

Figure 2 : L'adressage multicast (communication de type 1 vers n).

- Une adresse de type **anycast** officialise la proposition faite pour IPv4 dans le RFC 1546. Comme pour le multicast, une adresse anycast désigne un groupe d'interfaces. La différence est que le réseau va remettre le paquet anycast à un membre du groupe et non pas à tous comme pour le multicast. La sélection du membre qui réceptionnera le paquet est à la charge du réseau. Cela peut être le "plus proche" au sens du routage (nombre de sauts, RTD minimal…). Ce type d'adressage trouve son utilité par exemple lorsqu'il y a un service ou un contenu qui est répliqué sur plusieurs serveurs à travers l'Internet. Si les serveurs sont identifiés avec une adresse anycast, la communication du client ira vers le serveur le plus proche. La figure 3 illustre une communication avec une adresse anycast. Un seul des nœuds du groupe reçoit le paquet.

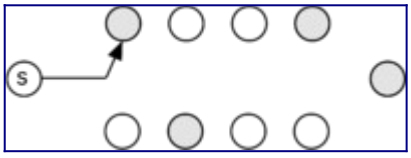

Figure 3 : L'adressage anycast (communication de type 1 parmi n).

Identification des types d'adresses

Le type d'une adresse IPv6 est identifié par ses bits de poids fort.

Type	Préfixe binaire d'identification	Notation IPv6
Non spécifié	`00...0`	`::/128`
Adresse de bouclage (Loopback)	`00...1`	`::1/128`
Multicast	`1111 1111`	`ff00::/8`
Unicast lien local	`1111 1110 10`	`fe80::/10`
Unique Local Unicast Address (ULA)	`1111 1101`	`fd00::/8`
Unicast globale (Plan d'adressage unicast global agrégé actuellement déployé)	`001`	`2000::/3` (soit toute adresse

commençant par 2 ou 3)

Certains types d'adresses sont caractérisés par leur préfixe RFC 3513. Le tableau suivant donne la liste de ces préfixes. La plage « réservée » du préfixe `0::/8` est utilisée pour les adresses spéciales (adresse indéterminée, de bouclage, mappée, compatible). On notera que plus de 70 % de l'espace disponible n'a pas été alloué, ce qui permet de conserver toute latitude pour l'avenir.

Préfixe IPv6	Allouer	Référence
`0000::/8`	Réservé pour la transition et loopback	RFC 3513
`0100::/8`	Réservé	RFC 3513
`0200::/7`	Réservé (ex NSAP)	RFC 4048
`0400::/6`	Réservé (ex IPX)	RFC 3513
`0800::/5`	Réservé	RFC 3513
`1000::/4`	Réservé	RFC 3513
`2000::/3`	Unicast Global	RFC 3513
`4000::/3`	Réservé	RFC 3513
`6000::/3`	Réservé	RFC 3513
`8000::/3`	Réservé	RFC 3513
`a000::/3`	Réservé	RFC 3513
`c000::/3`	Réservé	RFC 3513
`e000::/4`	Réservé	RFC 3513
`f000::/5`	Réservé	RFC 3513
`f800::/6`	Réservé	RFC 3513
`fc00::/7`	Unique Local Unicast	RFC 4193
`fe00::/9`	Réservé	RFC 3513
`fe80::/10`	Lien-local	RFC 3513
`fec0::/10`	Réservé	RFC 3879
`ff00::/8`	Multicast	RFC 3513

Une interface possédera généralement plusieurs adresses IPv6. En IPv4, ce comportement est exceptionnel ; il est banalisé en IPv6.

Les adresses anycast ne sont pas distinguées des adresses unicast de quelque portée (globale, locale, lien) que ce soit.

L'adressage unicast

Structure de l'adresse unicast

Le plan d'adressage agrégé actuellement en vigueur est défini dans le RFC 3587. Il s'inspire des recommandations de la politique d'allocation d'adresse des autorités régionales (RIR *Regional Internet Registry*), définie dans le document ripe-267 et dans le RFC 3177, qui est un plaidoyer pour un préfixe de taille fixe de 48 bits.

Les adresses IPv6 peuvent être agrégées avec des préfixes de longueur quelconque, de manière similaire aux mécanismes mis en œuvre dans les architectures CIDR (*Classeless InterDomain Routing*) d'IPv4.

Un nœud peut avoir une connaissance minimale de la structuration interne de l'adresse, en fonction de son rôle dans l'interconnexion. Un hôte ou un routeur n'a ainsi pas la même vision de la structure de l'adresse. Au minimum, un nœud peut considérer l'adresse unicast comme un simple mot binaire de 128 bits, sans aucune structure particulière telle que présentée dans la figure 4.

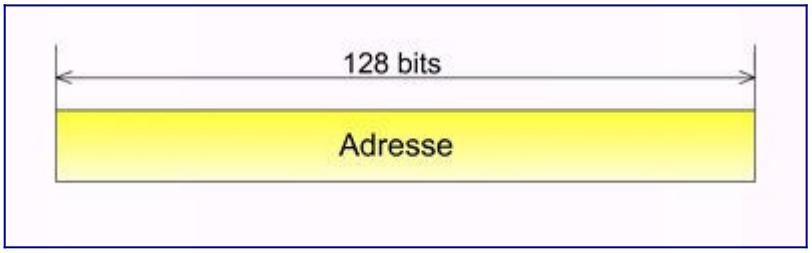

Figure 4 : Structure minimale de l'adresse IPv6.

Un premier niveau de hiérarchisation découpe l'adresse en deux parties logiques : un préfixe réseau/sous-réseau, qui sera utilisé pour acheminer le paquet à travers le réseau, et un identifiant d'interface qui sera utilisé sur le dernier saut pour remettre le paquet à l'interface de destination. Ceci est représenté dans la figure 5. En pratique, chaque partie a une longueur de 64 bits comme l'analyse le RFC 7421.

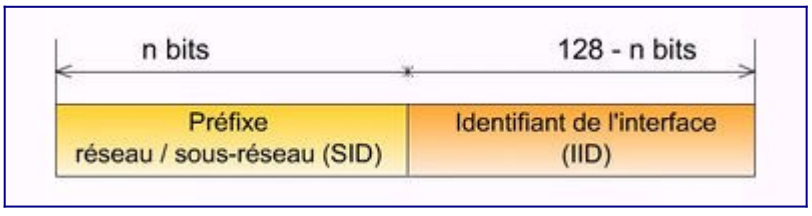

Figure 5 : Hiérarchisation à deux niveaux logiques.

Différents types d'adresse unicast

L'adresse non spécifiée

L'adresse `0:0:0:0:0:0:0:0` ou `::/128` est définie comme l'adresse non spécifiée. Elle ne doit jamais être affectée à un nœud. Elle indique l'absence d'adresse. Elle est utilisée comme adresse source par les paquets d'initialisation lors de l'auto-configuration d'une station. Elle ne doit jamais être utilisée comme adresse de destination d'un paquet.

L'adresse de bouclage (loopback)

L'adresse unicast `0:0:0:0:0:0:0:1` ou `::1/128` est appelée adresse de bouclage (loopback). Elle est équivalente à l'adresse 127.0.0.1 d'IPv4. Elle est utilisée par un nœud pour s'envoyer des paquets à lui-même. Elle ne doit jamais être affectée à une interface. Elle est considérée comme ayant une étendue de type "lien-local" et doit être vue comme une adresse unicast de "lien-local" de l'interface virtuelle de bouclage (*loopback interface*). Elle ne doit jamais être utilisée comme adresse source ou destination d'un paquet circulant sur le réseau ou, plus exactement, un paquet circulant hors de la machine. Un paquet reçu sur une interface avec une telle adresse de destination doit être détruit.

Les adresses unicast globales (GUA : Global Unicast Address)

Il s'agit des adresses globalement routables sur l'Internet V6. Elles sont communément qualifiées « d'adresses publiques ». Les adresses unicast globales sont issues du plan d'adressage agrégé, proposé dans le RFC 3587. Elles sont identifiées par le préfixe binaire `0b0010`[1], soit `2000::/3` en notation IPv6. Toute adresse IPv6 commençant par 2xxx:: ou 3xxx:: est donc une adresse unicast globale.

Le RFC 3587 définit la structure d'adressage IPv6 définie dans le RFC 3513 en précisant les tailles de chacun des blocs. Il est géré hiérarchiquement de la même manière que CIDR en IPv4. La figure 6 présente les trois niveaux de hiérarchie :

- une topologie publique (appelée *Global Prefix*) codée sur 48 bits, allouée par le fournisseur d'accès ;
- une topologie de site codée sur 16 bits (appelée *Subnet ID*). Ce champ permet de coder les numéros de sous-réseau du site ;
- un identifiant d'interface sur 64 bits (appelé *Interface ID*) distinguant les différentes machines sur le lien.

Figure 6 : Format général de l'adresse unicast globale.

À part le préfixe `2002::/16` qui est réservé au mécanisme de transition 6to4, cet espace est géré hiérarchiquement comme pour IPv4. L'IANA délègue aux 5 autorités régionales (RIR) des préfixes actuellement de longueur 12[2] qui les redistribuent aux ISP de leur région. Suivant leur taille, les opérateurs reçoivent un préfixe plus ou moins long.

Il est maintenant admis que le préfixe attribué par un opérateur à ses clients peut également être un /56. En effet, si l'on garde l'attribution de préfixe de longueur 48 pour les sites terminaux, et que l'on intègre les réseaux domotiques, les opérateurs peuvent justifier d'un besoin important d'adresses que les autorités régionales ne peuvent leur refuser.

Nota : quelques préfixes du plan d'adressage agrégé du RFC 3587 ont un usage réservé. Ils sont répertoriés parmi les préfixes réservés répertoriés dans le registre du RFC 6890 (*Special-*

Purpose IP Address Registries) complété du RFC 8190 (*Updates to the Special-Purpose IP Address Registries*).

Adresses à usage documentaire

Le RFC 3849 spécifie que le préfixe 2001:db8::/32 est réservé pour les usages documentaires. Il peut être utilisé pour les exemples dans les documentations des équipements ou les livres et documents de formation. Dans ce document, il est ainsi largement utilisé. La version précédente du protocole (IPv4) ne disposait pas initialement d'un tel préfixe ; ce qui pouvait poser des problèmes lorsque les documentations des équipements mentionnaient des exemples d'adresse que des administrateurs distraits ou maladroits saisissaient telles quelles sur leurs équipements car ces adresses étant valides, elles pouvaient être effectivement routées sur l'Internet. En IPv6, ce préfixe 2001:db8::/32 réservé pour cet usage n'est théoriquement par routé sur l'Internet public par les opérateurs. Depuis 2010, le RFC 5737 a complété le dispositif de documentation en spécifiant trois préfixes IPv4 à utiliser pour la documentation : 192.0.2.0/24 (TEST-NET-1), 198.51.100.0/24 (TEST-NET-2) et 203.0.113.0/24 (TEST-NET-3).

- Le préfixe `2002::/16` est réservé au mécanisme d'intégration dit "tunnel 6to4" *(Ce mécanisme maintenant considéré déprécié a été supplanté par le mécanisme 6rd. Les mécanismes d'intégration seront présentés dans la séquence 4).*
- **Le préfixe `2001:db8::/32` est réservé pour la documentation** (RFC 3849). Ces adresses ne sont théoriquement pas routés par les opérateurs sur l'Internet public.
- Le préfixe `2001:5::/32` est réservé par le RFC 7954 (*Locator/ID Separation Protocol* (LISP) *Endpoint Identifier (EID) Block*) dans le cadre du protocole expérimental LISP, visant à séparer les fonctions de localisation et d'identification des adresses.
- Le préfixe `2001:10::/28` réservé par le RFC 4843 ORCHID (*Overlay Routable Cryptographic Hash Identifiers*), protocole visant à séparer les fonctions de localisation et d'identification des adresses, déprécié au profit d'ORCHIDv2
- Le préfixe `2001:20::/28` réservé par le RFC 7343 ORCHIDv2 (*Overlay Routable Cryptographic Hash Identifiers* Version 2), protocole visant à séparer les fonctions de localisation et d'identification des adresses.
- Le préfixe `2001:1::1/128` adresse anycast du protocole PCP (*Port Control Protocol*) réservé par le RFC 7723 (*Port Control Anycast Address*).
- Le préfixe `3ffe::/16` était le préfixe des adresses du réseau expérimental 6bone qui a symboliquement été stoppé le 6 juin 2006 (06/06/06). Ces adresses sont donc aujourd'hui dépréciées.

Le plan agrégé `2000::/3` a été découpé en plusieurs plages d'adresses qui sont allouées par l'IANA aux différents RIR (Registres Internet Régionaux). Les RIR gèrent les ressources d'adressage IPv4 et IPv6 dans leur région (au niveau mondial). L'IANA alloue des blocs de taille /23 à /12 dans l'espace unicast global (`2000::/3`) aux cinq RIR. Ces derniers les allouent à leur tour aux LIR (fournisseurs d'accès à internet) sous forme de blocs de taille minimale de /48. Les RIR peuvent choisir de subdiviser leur bloc /23 en 512 blocs /32, typiquement un par LIR. Le LIR peut à son tour assigner 65536 blocs /48 à ses clients, qui disposent alors chacun de 65536 réseaux /64.

La plage `2001::/16` du plan 0x2::/3 (001) avait été initialement attribuée pour l'adressage agrégé des RIR (*Regional Internet Register*). Cette plage a ensuite été étendue au fur et à mesure des besoins. La version actualisée du découpage du plan d'adressage agrégé est disponible auprès de l'IANA[2].

La figure 7 représente un exemple concret : le plan d'adressage IPv6 de Renater, le réseau national de l'enseignement et de la recherche, fournisseur d'accès de l'enseignement supérieur français :

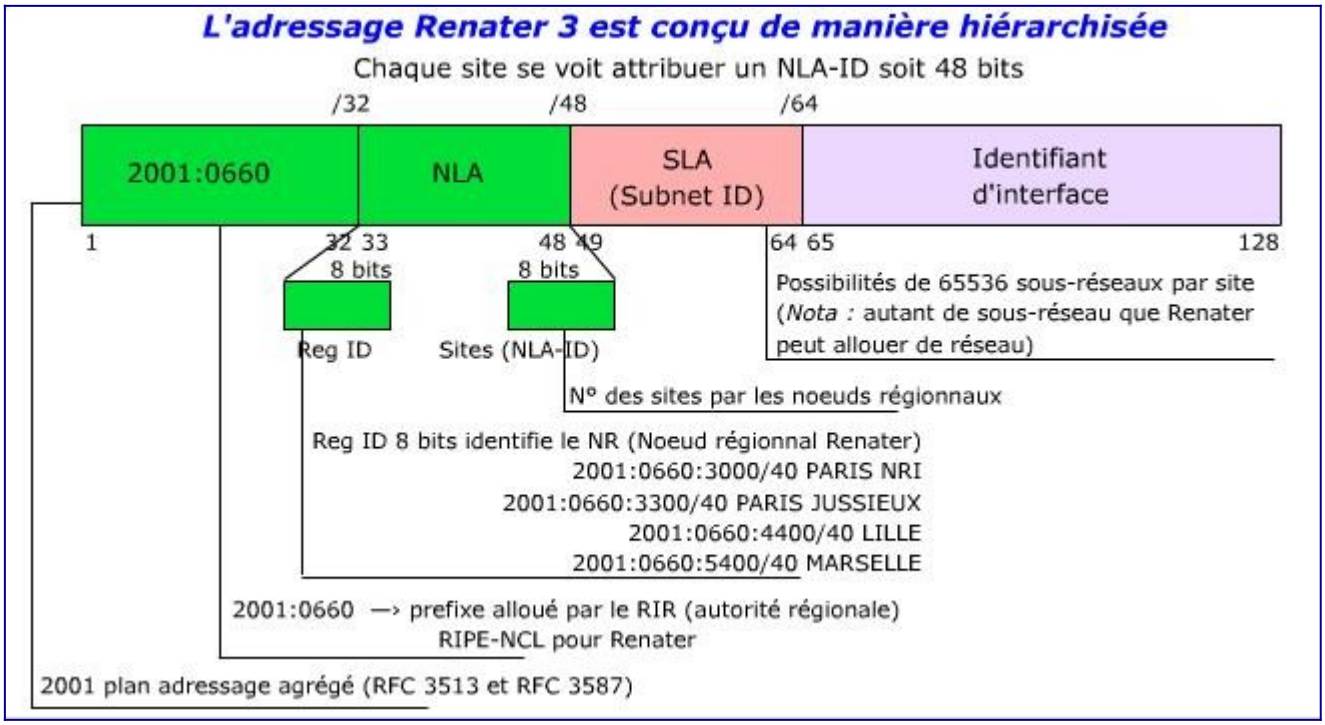

Figure 7 : Format de l'adressage Renater (Réseau NAtional de l'Enseignement et de la Recherche).

Les adresses unicast locales

Il y a deux types d'adresse unicast qui sont utilisées localement :

- les adresses locales de lien, dites "lien-local" que nous noterons aussi LLA (*Link Local Address*) ;
- les adresses unicast locales uniques notées ULA (*Unique Local unicast Address*).

Les adresses locales de lien (LLA : *Link Local Address*)

Les adresses "lien-local", sont des adresses dont l'étendue de validité est restreinte au lien ou au domaine de diffusion de niveau 2 (domaine de *broadcast* comme celui défini pour un VLAN (*Virtual Local Area Network*)). Que ce soit par un lien ou par un domaine de diffusion, les interfaces réseaux sont directement connectées entre elles. Elles sont dites voisines. La communication entre 2 interfaces voisines s'effectue sans aucun routeur intermédiaire. Par exemple, les deux extrémités d'une liaison PPP ou d'un tunnel, ou les machines connectées sur un même domaine de diffusion Ethernet (VLAN Ethernet) sont voisines et peuvent communiquer directement. Les adresses "lien-local" sont analogues aux adresses APIPA[3]

(*Automatic Private Internet Protocol Addressing*) d'IPv4 décrites dans le RFC 3927 (préfixe IPv4 réservé pour cet usage : 169.254.0.0/16).

Les adresses "lien-local" sont automatiquement configurées à l'initialisation de l'interface afin que la communication entre nœuds voisins puisse se faire. Elles sont utilisées par les protocoles de configuration d'adresse globale, de découverte de voisins et de découverte de routeurs. Elles doivent être uniques sur leur étendue, un protocole de détection de duplication d'adresse permet de s'en assurer. Par contre, la duplication d'une adresse "lien-local" entre deux liens différents est autorisée.

Ces adresses sont "non routables". Ainsi, un routeur ne doit en aucun cas retransmettre un paquet ayant pour adresse source ou destination une adresse de type "lien-local".

La portée restreinte de ces adresses les limite, dans la pratique, à un usage de démarrage automatique (*bootstrap*) et aux mécanismes de configuration automatique. Leur usage ne devrait pas être généralisé dans les applications.

La figure 8 représente le préfixe d'identification qui est `fe80::/10`. L'adresse "lien-local" a le format suivant : préfixe `fe80::/64` accolé au 64 bits de l'identifiant d'interface, généralement dérivé de l'adresse MAC de l'interface Ethernet. Cela ne pose pas de problème de respect de la vie privée car, contrairement aux adresses globales, les adresses "lien-local" ne sortent jamais du réseau où elles sont utilisées.

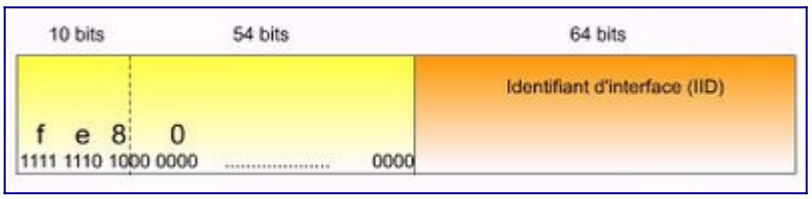

Figure 8 : Format de l'adresse lien-local.

Nota : *Une adresse "lien-local" (ou multicast) n'indique pas intrinsèquement l'interface de sortie puisque toutes les interfaces partagent le même préfixe fe80::/10. Il faut donc indiquer, de manière explicite, sur quelle interface doivent être émis les paquets. Sur certains systèmes d'exploitation (BSD, Mac OS, Windows), il est possible de la spécifier en ajoutant à la fin de l'adresse le nom de l'interface voulue, précédé du caractère "%". Sous Linux, un argument de commande réseau, généralement -I permet de la désigner.*

Les adresses locales uniques (ULA : *Unique Local unicast Address*)

Le RFC 4193 définit un nouveau format d'adresse unicast : les adresses uniques locales (ULA : *Unique Local unicast Address*). Dans leur usage, elles sont analogues aux adresses privées IPv4 du RFC 1918. Elles sont couramment appelées adresses privées (à l'inverse des adresses unicast globales dites publiques).

Ces adresses sont restreintes à un site unique et destinées à une utilisation locale. Elles sont routables à l'intérieur d'un espace privatif (réseau local de campus, réseau d'entreprise, réseau

domestique...) mais ne peuvent pas en sortir. Elles sont filtrées par les fournisseurs d'accès et ne peuvent donc pas être routées sur l'Internet public. La longueur du préfixe étant de 48 bits, elles peuvent se manipuler comme des adresses globales, avec un identifiant de sous-réseau (SID) sur 16 bits et un identifiant d'interface (IID) sur 64 bits.

Les adresses uniques locales sont créées en utilisant un identifiant global généré pseudo-aléatoirement selon l'algorithme défini dans le RFC 4193. La figure 9 indique que ces adresses suivent le format suivant :

- Prefix (7 bits) : `fc00::/7` préfixe identifiant les adresses IPv6 locales (ULA) ;
- L (1 bit) : positionné à 1, le préfixe est assigné localement ; la valeur 0 est réservée pour une utilisation future (dans la pratique, les adresses ULA en usage actuellement sont donc identifiées par le préfixe `fd00::/8`) ;
- Global ID (40 bits) : identifiant global utilisé pour la création d'un préfixe unique (*Globally Unique Prefix*) ;
- Subnet ID (16 bits) : identifiant d'un sous-réseau à l'intérieur du site ;
- Interface ID (64 bits) : l'identifiant d'interface permet de distinguer les différentes machines sur le lien.

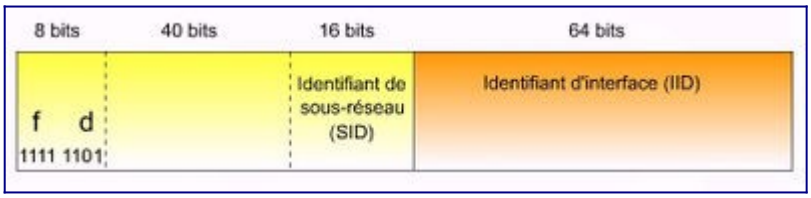

Figure 9 : Format de l'adresse unicast locale.

Ce type d'adresse permet d'isoler la numérotation externe et interne. En IPv4, l'utilisation d'un préfixe privé issu du RFC 1918 (comme `10.0.0.0/8`) évite à un site de renuméroter son réseau s'il change de fournisseur d'accès. Un NAT (que nous appellerons NAT44 dans la suite de ce document) permet de passer de l'adressage privé à l'adressage public.

Avec les adresses de type ULA, il est possible de reproduire ce comportement en IPv6. Un dispositif, en bordure de réseau, va convertir le préfixe privé en préfixe public. Cet équipement, initialement appelé NAT66, a été renommé NPTv6 (*Network Prefix Translation*) car il ne possède pas les mêmes limitations que le NAT d'IPv4 du fait qu'il n'intervient pas au niveau de la couche de transport.

Comme pour le RFC 1918 d'IPv4, l'objectif est de permettre un adressage à usage privatif non routé sur l'infrastructure publique. Mais, à la différence du RFC 1918, où le risque de collision élevé est problématique en cas de connexion de deux sites utilisant ces adresses (lors de fusions d'entreprises par exemple), il s'agit de générer des préfixes quasi uniques. Dans un espace réservé, `fc00::/7`, le site qui souhaite des adresses quasi uniques tire un préfixe de 48 bits au hasard, suivant l'algorithme décrit dans le RFC 4193 en se basant sur l'heure courante et une adresse MAC d'une de ses interfaces. La probabilité de collision est donc très faible, vue la taille de l'espace d'adressage d'IPv6.

Ces adresses sont dites locales, et ne doivent pas être routées sur l'Internet global. Elles sont routables sur un espace limité tel un site. Elles peuvent également être routées entre un

nombre limité de sites (sur la même aire interne d'un IGP, comme OSPF, ou au travers de tunnels point à point reliant les sites). Elles ont les caractéristiques suivantes :

- préfixe globalement unique (très forte probabilité d'unicité) ;
- un préfixe bien connu `fc00::/7` facilitant le filtrage aux frontières du site ;
- limitation des conflits ou des opérations de réadressage lors de la fusion de sites où l'interconnexion privée de sites ;
- indépendance des préfixes vis-à-vis des fournisseurs d'accès ou des opérateurs ;
- indépendance vis-à-vis des applications : elles s'utilisent de la même manière que les adresses unicast globales ;
- en cas de débordement géographique accidentel (mauvaise configuration de l'annonce des routeurs ou des filtres, affichage accidentel dans un DNS public), l'unicité garantit l'absence de conflit avec d'autres adresses.

L'identifiant global de 40 bits ne doit pas être choisi de manière séquentielle ou selon un algorithme permettant de déduire un préfixe en fonction des autres préfixes du site. Il ne doit pas, non plus, être choisi par facilité mnémotechnique en *hexspeak*, amusement consistant a générer des jeux de mots pour les codes hexadécimaux en mixant les lettres hexadécimales (a à f) et les chiffres 1 (pour 'i' ou 'l'), 0 (pour 'o'), 5(pour 's'), 6 ou 9 (pour 'g'), 7 (pour 't') ; les plus connus étant 'bad:f00d' « bad food », '600d:cafe' « good cafe », 'dead:beef' « dead beef », ou encore 'defe:ca7e:d « ... », et bien d'autres (source http://en.wikipedia.org/wiki/Hexspeak).

Le préfixe de l'adresse IPv6 locale unique est créée en s'appuyant sur un mécanisme pseudo-aléatoire. Le RFC 4193 propose l'algorithme suivant :

1. prendre l'heure courante dans le format 64 bits du protocole NTP ;
2. prendre un identifiant EUI-64, au besoin dérivé de l'adresse MAC, de l'une des interfaces de l'équipement générant le préfixe ;
3. concaténer l'heure et l'identifiant d'interface pour créer une clé ;
4. calculer l'empreinte SHA-1 (digest) de 160 bits de cette clé ;
5. prendre les 40 bits de poids faible de l'empreinte comme identifiant global de 40 bits ;
6. préfixer l'identifiant global avec le préfixe fc00::/7 et positionner le bit L (8^e bit de poids fort) à 1. Dans la pratique, les préfixes ULA débutent donc par « fd ».

L'outil en ligne disponible à l'URL https://cd34.com/rfc4193/, peut vous aider à générer un préfixe /48 conforme en utilisant une des adresses MAC Ethernet de votre machine. Le site https://ula.ungleich.ch en plus de créer un préfixe aléatoirement, l'enregistre dans une base de données.

Ces préfixes ne devraient pas pouvoir être agrégés afin de renforcer la « non-routabilité » globale sur l'Internet. Par défaut, l'étendue de ces adresses est globale ; ce qui signifie qu'elles ne souffrent pas de l'ambiguïté levée par l'adresse site-local (un réseau ou un ensemble de réseaux interconnectés dans un site ou un campus). La limite de « routabilité » est fixée au site et à toutes les routes explicitement définies avec d'autres sites privés (soit dans la même aire d'IGP, soit au travers de tunnels). Pour les protocoles de routage extérieur (EGP *Exterior Gateway Protocol*), tel BGP, mis en œuvre par les fournisseurs d'accès, la consigne est

d'ignorer la réception et l'annonce de préfixes `fc00::/7`.

Portée de l'adresse unicast

On retiendra que les adresses IP courantes de communication pair à pair, dites unicast, supportent différentes portées de communication. La portée d'une adresse unicast qualifie l'étendue de validité et délimite donc sa "routabilité".

Cette portée peut être globale. Les adresses unicast globales (GUA), également qualifiées d'"adresses publiques", sont ainsi routables à l'échelle du réseau public mondial Internet.

Inversement, la portée des adresses locales (ULA couramment dénommées "adresses privées") sera limitée au périmètre de l'architecture privative auquel elle s'applique. Ces adresses locales sont routables sur l'étendue de la topologie privative. Elles n'ont pas de validité ni de signification sur l'Internet public.

Dans le cas des adresses locales de lien (LLA), cette portée est restreinte au seul lien ou domaine de diffusion auquel est attachée l'interface de communication. Une adresse LLA est donc non routable. Les paquets portant une telle adresse sont "confinés" au lien et ne permettent qu'une communication avec le voisinage direct.

L'administrateur du réseau doit connaître ces portées lors des choix de stratégie d'attribution des adresses aux équipements.

L'adressage multicast

Les adresses de multidiffusion dites multicast, également appelées adresses de groupe, permettent de communiquer avec un ensemble d'interfaces. Le paquet émis avec une destination multicast sera délivré par le réseau à chacune des interfaces abonnées au groupe de multicast. C'est une manière efficace de diffuser de la donnée.

Sur Internet, l'usage du multicast ne s'est pas banalisé et n'est pas majoritaire. Cependant, les fonctions de contrôle et de découverte du voisinage du protocole IPv6, que nous aborderons dans une prochaine séquence, font usage du multicast. Nous allons donc nous attarder sur la structuration de ces adresses et identifier les groupes réservés à la gestion d'IPv6.

Structure de l'adresse multicast

Les adresses multicast IPv6 sont dérivées du préfixe `ff00::/8`. L'identification du groupe est faite sur 112 bits ; ce qui donne un potentiel d'environ 5 x 10^33 groupes différents. Une portée spécifique est associée à une adresse multicast afin de limiter la propagation du trafic multicast. Le format général est présenté par la figure 1 [RFC 4291].

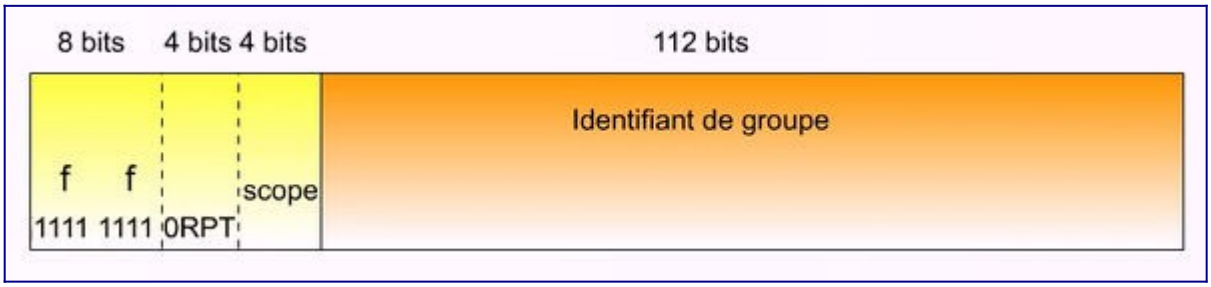

Figure 1 : Format général de l'adresse multicast.

Le champ `drapeaux` (*flags*) spécifie le type d'adresses multicast IPv6 qui seront décrites dans la suite du document. Le champ `drapeaux`, d'une longueur de 4 bits, suit les 8 bits d'identification. Ce champ comporte les drapeaux suivants :

- le bit T (*Transient*) indique le mode d'obtention de l'adresse multicast. La valeur 0 signifie que l'adresse multicast est bien connue et est gérée par une autorité, en l'occurence l'IANA. La valeur 1 indique une adresse temporaire ou dynamiquement allouée ;
- le bit P indique une méthode de création reposant sur un préfixe unicast [RFC 3306] ;
- le bit R indique, pour les arbres de distribution partagée, que l'adresse du point de rendez-vous est contenue dans l'identifiant du groupe [RFC 3956] ;
- le bit de poids fort du champ `drapeaux` n'est pas encore attribué.

Le champ `étendue` (*scope*) limite la portée de la diffusion de l'adresse multicast IPv6. Avec ce champ, le confinement des datagrammes dans une zone déterminée est maîtrisé. Cette méthode est plus rigide mais plus précise que la première proposition du multicast d'IPv4, où la portée était limitée uniquement par le champ `durée de vie` (*Time To Live* (TTL)) du paquet. Les portées suivantes sont définies [RFC 7346] :

- 0 - reserved
- 1 - node-local
- 2 - link-local
- 3 - realm-local
- 4 - admin-local
- 5 - site-local
- 8 - organisation-local
- e - global
- f - reserved

Les 112 bits restants portent l'identifiant du groupe de diffusion. Suivant le mode de diffusion, il peut être structuré (cf. annexe de cette activité).

Dans l'exemple suivant, l'identifiant de groupe prédéfini 101 a été réservé auprès du registre de l'IANA pour le protocole de distribution d'horloge NTP (*Network Time Protocol*). Ce protocole dispose d'une adresse de multicast valide quelque soit son étendue.

Adresse de multicast	Population concernée
`ff01::101`	Tous les serveurs NTP de la même interface (c.à.d. le même nœud) que

	l'émetteur ;
`ff02::101`	Tous les serveurs NTP du même lien que l'émetteur ;
`ff05::101`	Tous les serveurs NTP du même site que l'émetteur ;
`ff0e::101`	Tous les serveurs NTP de l'Internet.

Si des services tels que le protocole NTP ont une adresse de multicast quelque soit la portée, d'autres identifiant multicast prédéfinis ne sont valides que sur un nombre limité de portées et administrativement interdit pour les autres portées pour se prémunir des attaques en déni de service par inondation ou par bombardement massif en diffusion.

Adresses de multicast de voisinage nécessaires à la gestion d'IPv6

diffusion restreinte : tous les nœuds du lien

L'identifiant de groupe à la valeur réservée "1" concerne tous les nœuds. Il est limité aux étendues "interface locale" `ff01::1` et "lien local" `ff02::1`. Cette dernière correspond au *broadcast* restreint d'IPv4 (adresse 255.255.255.255). Les autres portées sont invalides pour se prémunir de dénis de services par inondation. On ne peut donc pas diffuser sur l'ensemble des nœuds de l'internet.

diffusion restreinte : tous les routeurs du lien

Le groupe d'identifiant multicast à la valeur réservée "2" diffuse à l'ensemble des routeurs. Il est limité aux étendues "interface locale" `ff01::2`, "lien local" `ff02::2` et "site local" `ff05::2`. Là aussi, on ne peut pas diffuser sur l'ensemble des routeurs de l'internet.

diffusion restreinte : l'adresse multicast sollicité

Enfin, une dernière adresse de diffusion particulière nécessaire à la gestion d'IPv6 est l'adresse de "multicast sollicité".

L'adresse de "multicast sollicité" (*Solicited-node address*) est un type d'adresse multicast prédéfinie. IPv6 interdit l'utilisation de la diffusion généralisée (*broadcast*) lorsque le multicast est disponible. Ainsi, les protocoles de découverte de voisins (*Neighbor Discovery*), chargés de faire la correspondance entre les adresses IPv6 et les adresses MAC (à l'instar d'ARP en IPv4) doivent utiliser une adresse multicast. Pour être plus efficace, au lieu d'utiliser l'adresse `ff02::1` (tous les équipements sur le lien), l'utilisation des adresses de "multicast sollicité" permet de réduire considérablement le nombre d'équipements qui recevront la requête de découverte de voisins.

L'adresse de "multicast sollicité" se construit automatiquement à partir d'une adresse IPv6 unicast (ou anycast) en concaténant le préfixe réservé `ff02::1:ff00:0 /104` aux 24 bits de poids faible de l'adresse unicast ou anycast. La figure 7 illustre le format *Solicited-node address*.

Un équipement, à partir de chacune de ses adresses IPv6 (unicat et anycast), construit une

adresse de "multicast sollicité" et écoute les paquets émis vers cette adresse. Les autres stations sur le même lien (ou domaine de diffusion de niveau 2 : VLAN), connaissant son adresse IPv6 mais ignorant son adresse MAC, peuvent utiliser l'adresse de "multicast sollicité" pour le joindre. Ces adresses sont utilisées par les protocoles de détection d'adresse dupliquée et de découverte de voisins, qui seront abordés ultérieurement.

Plusieurs équipements sur le lien peuvent avoir la même adresse de "multicast sollicité". Mais, dans la pratique, la probabilité de trouver sur le même lien physique deux équipements avec les trois derniers octets de l'identifiant d'interface identiques est très faible. Cela permet donc de limiter le nombre d'équipements qui traiteront la requête de sollicitation de voisins. Ces adresses permettent de ne plus utiliser la diffusion généralisée (adresse MAC ff:ff:ff:ff:ff:ff) qu'utilise le protocole ARP en IPv4. Pour une station donnée, une adresse de "multicast sollicité" peut regrouper plusieurs adresses IPv6, par exemple l'adresse lien-local et l'adresse "unicast globale" si cette dernière est construite à partir de l'identifiant d'interface dérivé de l'adresse MAC de la carte Ethernet.

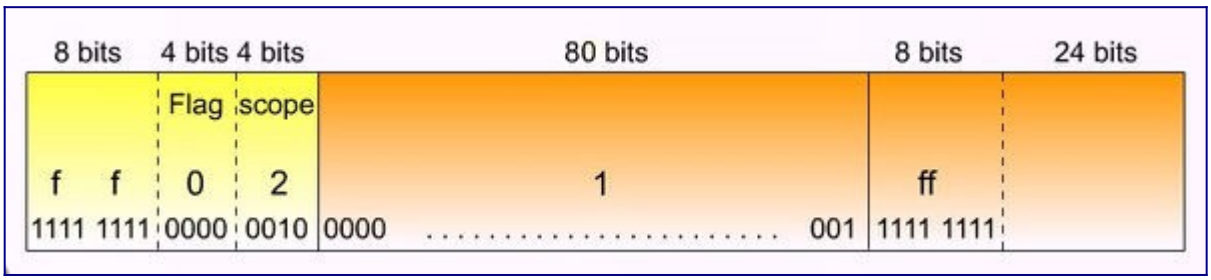

Figure 7 : Format de l'adresse "multicast sollicité".

conclusion

Au cours de cette activité, nous avons abordé les différents types d'adresse en usage sur les réseaux IP en général et l'internet en particulier. En IPv6, ces différents types d'adresse sont immédiatement identifiables par lecture directe des premiers octets de poids fort de l'adresse. Reconnaître le type d'une adresse, son usage et sa portée, c'est-à-dire sa routabilité, est une compétence préalable au déploiement et à l'exploitation des réseaux afin de configurer correctement les différents équipements. Pour l'exploitant, les adresses clairement identifiées facilitent l'analyse des journaux système ou de flux capturés par les analyseurs de protocole lors des tâches d'administration de l'infrastructure. En terminant cette activité, vous disposez des fondamentaux nécessaires à la compréhension du fonctionnement du protocole et à sa mise en œuvre qui seront abordés dans les prochaines séquences d'activités.

Références bibliographiques

1. ↕ Notation binaire. Que signifie «0b».
2. ↑ 2.0 2.1 IANA. IPv6 Global Unicast Address Assignments
3. ↕ Wikipédia. Automatic Private Internet Protocol Addressing

Pour aller plus loin

RFC et leur analyse par S. Bortzmeyer :

- RFC 1516 Host Anycasting Service
- RFC 1918 Address Allocation for Private Internets Analyse
- RFC 3177 IAB/IESG Recommendations on IPv6 Address Allocations to Sites
- RFC 3513 Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3849 IPv6 Address Prefix Reserved for Documentation Analyse
- RFC 3879 Deprecating Site Local Addresses Analyse
- RFC 3927 Dynamic Configuration of IPv4 Link-Local Addresses Analyse
- RFC 4048 RFC 1888 Is Obsolete
- RFC 4193 Unique Local IPv6 Unicast Addresses Analyse
- RFC 4548 Internet Code Point (ICP) Assignments for NSAP Addresses
- RFC 6598 IANA-Reserved IPv4 Prefix for Shared Address Space Analyse
- RFC 6890 Special-Purpose IP Address Registries Analyse
- RFC 7343 An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers Version 2 (ORCHIDv2) Analyse
- RFC 7421: Analysis of the 64-bit Boundary in IPv6 Addressing Analyse
- RFC 7723 Port Control Protocol (PCP) Anycast Addresses Analyse
- RFC 7954 Locator/ID Separation Protocol (LISP) Endpoint Identifier (EID) Block Analyse
- RFC 7955 Management Guidelines for the Locator/ID Separation Protocol (LISP) Endpoint Identifier (EID) Block Analyse
- RFC 8190 Updates to the Special-Purpose IP Address Registries Analyse

Annexe : Le multicast en IPv6

Introduction

Les adresses multicast, également appelées adresses de groupe, sont un élément important dans la proposition Multicast IP. Le fonctionnement du multicast en IPv6 reprend les principes énoncés pour IPv4. Ces principes ont été posés dans les années 1990[1]. Multicast IP est présenté en détail par cet article de Cisco [2]. Le lecteur est invité à consulter cet article pour y découvrir le fonctionnement de ce mode de communication. Nous allons voir dans cette activité comment sont formatées les adresses IPv6 multicast[3] uniquement. Cette activité n'aborde que partiellement le fonctionnement du multicast.

Communication multicast

Une communication multicast est une communication dans laquelle un paquet émis peut être reçu par plusieurs récepteurs, quelque soit leur localisation. Dans le modèle multicast IPv6, les récepteurs forment un groupe et celui-ci est identifié par une adresse dite de multicast.

Comparé aux communications point à point (*unicast*), le multicast évite la duplication des paquets de données au niveau de la source, et minimise l'utilisation de la bande passante au niveau du réseau. C'est une manière efficace de communiquer avec un ensemble de machines. De plus, il offre un service insensible à l'augmentation du nombre et de la localisation des membres d'un groupe. Le multicast peut être utilisé pour la distribution de logiciels, la téléconférence, les applications d'enseignement à distance, la radio ou la télévision sur Internet, les simulations interactives distribuées, les jeux multimédia interactifs, les applications militaires, etc.

Le service de communication multicast se rend selon 2 modèles :

- le modèle ASM (*Any-Source Multicast*) : avec ce modèle, une source quelconque peut émettre des données à un groupe. Ce modèle s'applique par exemple dans le cas de visioconférences avec de nombreux participants qui ne sont pas connus à l'avance ;
- le modèle SSM (*Source-Specific Multicast*) [RFC 3569] : avec ce modèle, les sources sont connues à l'avance et les récepteurs peuvent restreindre les réceptions d'un groupe pour une source donnée. Ce modèle s'applique par exemple à la diffusion de la télévision ou radio sur Internet, où il n'y a qu'une seule source connue de tous.

Les étapes suivantes interviennent dans l'établissement d'une session multicast IPv6 :

- choix de l'adresse multicast pour la session ;
- description et annonce de la session multicast à tous les participants ;
- gestion des membres du groupe sur le lien-local : elle est réalisée par le protocole MLD (*Multicast Listener Discovery*) ;
- construction de l'arbre multicast : elle est assurée par le protocole de routage multicast PIM (*Protocol Independant Multicast*).

Le fonctionnement détaillé du multicast dépasse le cadre de cette présentation. Cette activité dans cette séquence ne présente que le format des adresses IPv6 multicast et les mécanismes permettant l'allocation des adresses multicast.

Formats des adresses multicast IPv6

Pour initier une session multicast, le groupe de récepteurs intéressés, appelé aussi groupe multicast, doit être identifié par une adresse IP multicast. L'allocation des adresses multicast doit se faire en garantissant l'unicité de l'adresse multicast à un groupe. Ainsi, il y a des adresses qui sont constituées par une autorité centrale. Dans ce cas, des adresses permanentes sont attribuées à des groupes bien connus. Enfin, pour des applications particulières, des adresses multicast peuvent être constituées dynamiquement et de manière temporaire. Nous allons décrire dans ce paragraphe le format des adresses multicast dans ces deux cas de figure.

Format général

Les adresses multicast IPv6 sont dérivées du préfixe `ff00::/8`. L'identification du groupe est faite sur 112 bits ; ce qui donne un potentiel d'environ 5 x 10^33 groupes différents. Une portée

spécifique est associée a une adresse multicast afin de limiter la propagation du trafic multicast. Le format général est présenté par la figure 1 [RFC 4291].

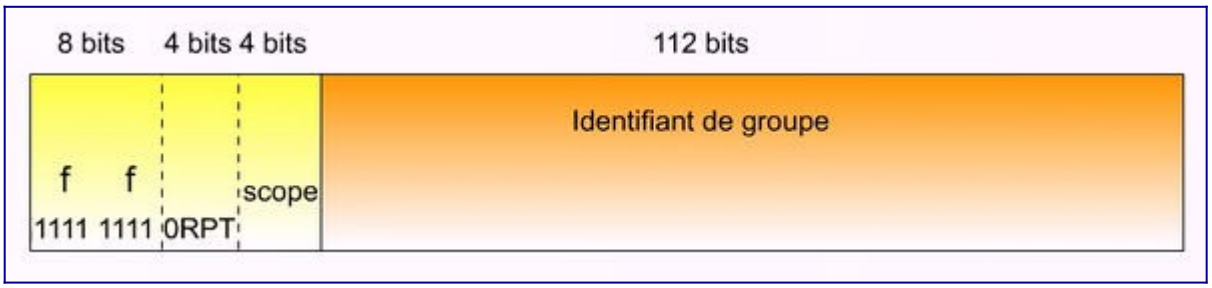

Figure 1 : Format général de l'adresse multicast.

Le champ `drapeaux` (*flags*) spécifie le type d'adresses multicast IPv6 qui seront décrites dans la suite du document. Le champ `drapeaux`, d'une longueur de 4 bits, suit les 8 bits d'identification. Ce champ comporte les drapeaux suivants :

- le bit T (*Transient*) indique le mode d'obtention de l'adresse multicast. Quand la valeur est à 0, elle signifie que l'adresse multicast est bien connue et est gérée par une autorité, en l'occurence l'IANA. La valeur 1 indique une adresse temporaire ou dynamiquement allouée ;
- le bit P indique une méthode de création reposant sur un préfixe unicast [RFC 3306] ;
- le bit R indique, pour les arbres de distribution partagée, que l'adresse du point de rendez-vous est contenue dans l'identifiant du groupe [RFC 3956] ;
- le bit de poids fort du champ `drapeaux` n'est pas encore attribué.

Le champ `étendue` (*scope*) limite la portée de la diffusion de l'adresse multicast IPv6. Avec ce champ, le confinement des datagrammes dans une zone déterminée est maîtrisé. Cette méthode est plus rigide mais plus précise que la première proposition du multicast d'IPv4, où la portée était limitée uniquement par le champ `durée de vie` (*Time To Live* (TTL)) du paquet. Les portées suivantes sont définies [RFC 7346] :

- 0 - reserved
- 1 - node-local
- 2 - link-local
- 3 - realm-local
- 4 - admin-local
- 5 - site-local
- 8 - organisation-local
- e - global
- f - reserved

Adresses multicast IPv6 permanentes

Une adresse multicast IPv6 avec le bit T du champ `drapeaux` à 0 correspond à une adresse multicast permanente, allouée par l'IANA. La figure 2 illustre cette adresse multicast permanente.

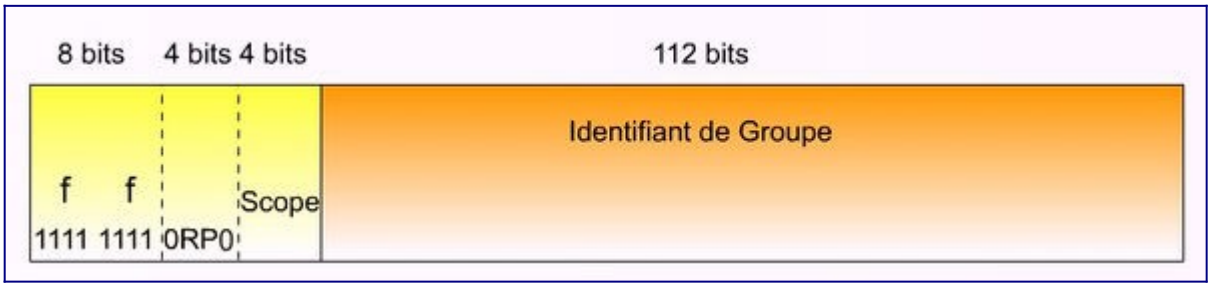

Figure 2 : Format de l'adresse multicast permanente.

Lorsque le multicast IPv6 sera déployé à grande échelle, certains organismes pourraient avoir des émissions permanentes. Des chaînes de télévision ou stations de radio pourront par exemple se voir attribuer des adresses permanentes par l'IANA dans le préfixe `ff00::/12`.

Le RFC 2375 définit déjà certaines adresses IPv6 multicast. Deux types d'adresses multicast permanentes sont à distinguer :

- des adresses correspondant à des services de niveau réseau (comme NTP, DHCPv6, cisco-rp-announce, SAP...) ;
- des adresses correspondant davantage à des services applicatifs commerciaux permanents comme la distribution des chaînes de télévision.

Le RFC 3307 définit les procédures pour l'allocation des adresses multicast permanentes. Une adresse multicast permanente a un sens quelque soit son étendue (*scope*). Son identifiant de groupe est réservé pour toutes les portées. Ainsi, l'identifiant 0x101 est réservé pour les serveurs NTP (*Network Time Protocol*).

Adresse de multicast	Population concernée
`ff01::101`	Tous les serveurs NTP de la même interface (c.à.d. le même nœud) que l'émetteur ;
`ff02::101`	Tous les serveurs NTP du même lien que l'émetteur ;
`ff05::101`	Tous les serveurs NTP du même site que l'émetteur ;
`ff0e::101`	Tous les serveurs NTP de l'Internet.

Cependant, par précaution, certains identifiants multicast prédéfinis ne sont valables que sur un nombre limité de portées. Exemple : les identifiants multicast relatifs au groupe des nœuds ou des routeurs sont limités aux portées lien-local ou site-local. D'autres, en général les services bien connus tels que NTP cité ci-dessus, sont valides pour toutes les portées. L'IANA tient un registre[4] de l'ensemble des adresses multicast réservées.

- L'identifiant de groupe « tout à zéro » est réservé quelque soit la portée et ne doit jamais être utilisé : `ff0x:0:0:0:0:0:0:0` avec x variant de '0' à 'f'.
- Le groupe d'identifiants multicast à 1 concerne tous les nœuds. Il est limité aux étendues (*scope*) interface-local et link-local. On ne peut donc pas diffuser sur l'ensemble des

nœuds de l'Internet (sage précaution car sinon, il aurait très facilement permis des attaques de type "déni de service" par bombardement massif en diffusion).

Adresse de mutlicast	Population concernée
`ff01::1`	Toutes les interfaces du nœud ;
`ff02::1`	Tous les nœuds sur le même lien que l'interface émettrice (correspond au broadcast 255.255.255.225 d'IPv4).

- Le groupe d'identifiants multicast à 2 concerne l'ensemble des routeurs. Il est limité aux étendues (*scope*) interface-local, link-local et site-local. On ne peut donc pas diffuser sur l'ensemble des routeurs de l'Internet (sage précaution "bis", pour limiter les attaques en "déni de service").

Adresse de multicast	Population concernée
`ff01::2`	Tous les routeurs du nœud ;
`ff02::2`	Tous les routeurs du lien ;
`ff05::2`	Tous les routeurs du site.

Adresses multicast IPv6 temporaires

Les adresses multicast temporaires sont des adresses multicast IPv6 dont le bit T est positionné à 1. À l'inverse des adresses multicast permanentes, une adresse multicast temporaire n'a de signification que dans la portée donnée. Exemple : l'adresse multicast site-local `ff15::999` sur un site n'a aucune relation avec un groupe utilisant la même adresse multicast sur un autre site. Il existe plusieurs types d'adresses temporaires : générales, dérivées d'un préfixe unicast IPv6, et par point de rendez-vous (Embedded-RP).

Adresses multicast temporaires générales

Ce sont des adresses avec tous les bits du champ `drapeaux` à 0 sauf le bit T positionné à 1. La figure 3 illustre ce format. Il n'y a pas de recommandation pour l'utilisation de ces adresses. Des scénarios d'utilisation peuvent être, par exemple, les visioconférences ponctuelles.

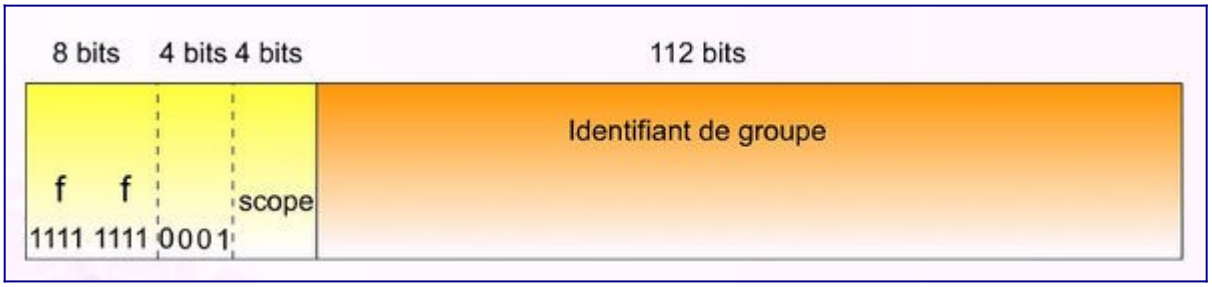

Figure 3 : Format général de l'adresse multicast temporaire.

Adresses multicast temporaires dérivées d'un préfixe unicast IPv6

Le RFC 3306 définit une méthode pour dériver une adresse multicast IPv6 à partir d'un préfixe unicast. La figure 4 représente ce format.

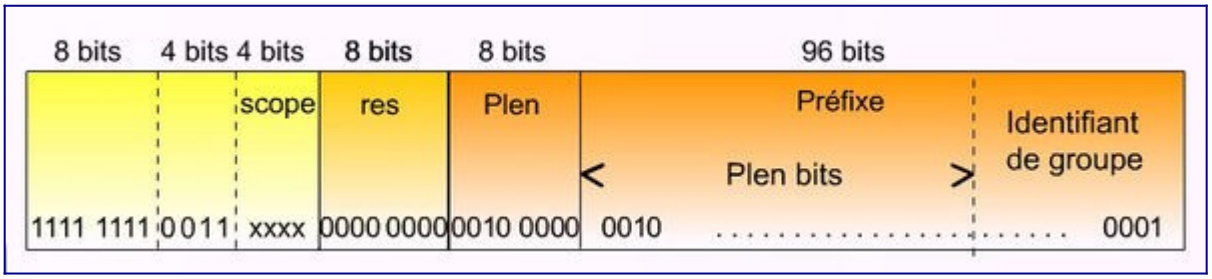

Figure 4 : Format de l'adresse multicast temporaire dérivée d'un préfixe unicast IPv6.

- `res` (*reserved*) : tous les bits de ce champ doivent être positionnés à `0`.
- `Plen` (*prefix length*) : ce champ contient la longueur du préfixe unicast utilisé pour en dériver une adresse multicast.
- `prefix` : ce champ contient la valeur du préfixe du réseau utilisé pour en dériver une adresse multicast.
- `group-ID` : ce champ de 32 bits contient l'identifiant de groupe.

Par exemple, une adresse multicast peut être dérivée du préfixe de RENATER (`2001:660::/32`). Le champ `prefix` prend la valeur `2001:0660`, et le champ `Plen`, la valeur `0x20` (32 en décimal). Les adresses multicast IPv6 à choisir seront de type `ff3x:20:2001:660::aabb:ccdd` ; `aabb:ccdd` étant le group-ID choisi dans l'exemple, et *x* une des valeurs valides de la portée (*scope*). Cette méthode permet la création potentielle de 2^32 adresses multicast par préfixe.

Adresses multicast *Embedded-RP*

Le RFC 3956 définit une méthode pour inclure l'adresse du RP (*Rendez-vous Point*) servant à la construction de l'arbre multicast dans l'adresse multicast IPv6. La figure 5 montre la structure d'une adresse multicast *embedded RP*.

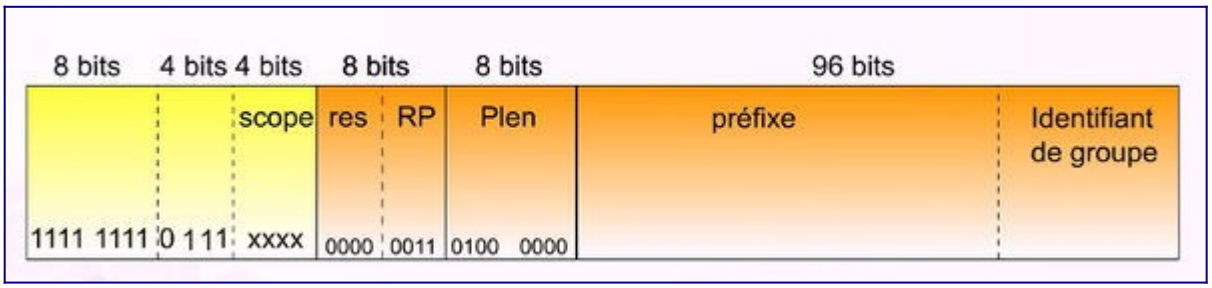

Figure 5 : Format de l'adresse multicast temporaire *embedded-RP*.

Ainsi, pour un point de rendez-vous qui possède l'adresse `2001:660:3307:125::3`, une adresse multicast correspondante peut être dérivée de la façon suivante :

- `res` (Reservé) : les 4 bits de ce champ sont positionnés à 0.
- `RPad` : ce champ contient les 4 derniers bits de l'adresse du RP. Dans cet exemple, RPad prend la valeur 3.

- `Plen` (Longueur du préfixe) : ce champ contient la longueur du préfixe réseau du RP à prendre en compte. Dans cet exemple, la valeur est de `0x40` (soit 64 en décimal).
- `prefix` (Préfixe) : ce champ contient le préfixe réseau du RP. Ici, cette valeur est `2001:660:3007:125`
- `group-ID` : ce champ de 32 bits contient l'identifiant de groupe, détaillé au chapitre "Identifiant de groupe".

Une adresse multicast dérivée de ce point de rendez-vous sera donc de la forme `ff7x:340:2001:660:3007:125:aabb:ccdd` ; `aabb:ccdd` étant le group-ID choisi dans cet exemple, et *x* une des valeurs valides de la portée (*scope*).

Les adresses multicast SSM

Les adresses SSM (*Source Specific Multicast*) sont décrites également dans le RFC 3306. Si le préfixe `ff3x::/32` a été réservé pour les adresses multicast SSM, seules les adresses dérivées du préfixe `ff3x::/96` doivent être utilisées dans un premier temps. Ce sont des adresses multicast basées sur le préfixe unicast où les champs `Plen` et `prefix` sont positionnés à 0. La figure 6 représente ce format.

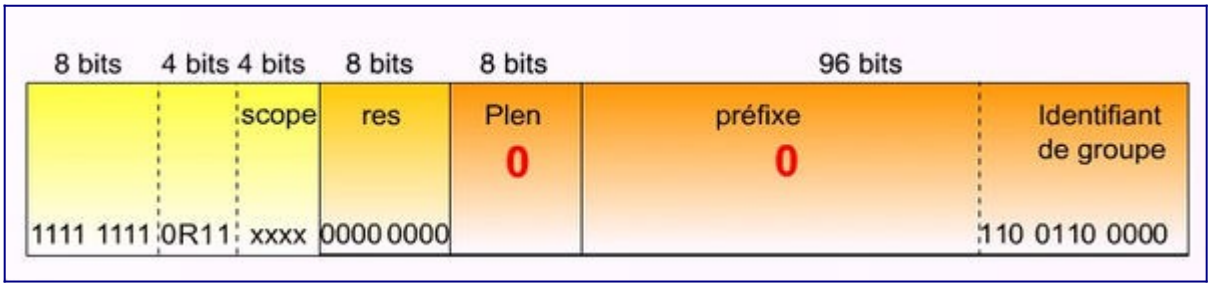

Figure 6 : Format de l'adresse multicast SSM.

Les adresses "multicast sollicité"

L'adresse de "multicast sollicité" (*Solicited-node address*) est un type d'adresse multicast prédéfinie. IPv6 interdit l'utilisation de la diffusion généralisée (*broadcast*) lorsque le multicast est disponible. Ainsi, les protocoles de découverte de voisins (*Neighbor Discovery*), chargés de faire la correspondance entre les adresses IPv6 et les adresses MAC (à l'instar d'ARP en IPv4) doivent utiliser une adresse multicast. Pour être plus efficace, au lieu d'utiliser l'adresse `ff02::1` (tous les équipements sur le lien), l'utilisation des adresses de "multicast sollicité" permet de réduire considérablement le nombre d'équipements qui recevront la requête de découverte de voisins.

L'adresse de "multicast sollicité" se construit automatiquement à partir d'une adresse IPv6 unicast (ou anycast) en concaténant le préfixe réservé `ff02::1:ff00:0 /104` aux 24 bits de poids faible de l'adresse unicast ou anycast. La figure 7 illustre le format *Solicited-node address*.

Un équipement, à partir de chacune de ses adresses IPv6 (*unicast* et *anycast*), construit une adresse de "multicast sollicité" et écoute les paquets émis vers cette adresse. Les autres stations sur le même lien (ou domaine de diffusion de niveau 2 : VLAN), connaissant son

adresse IPv6 mais ignorant son adresse MAC, peuvent utiliser l'adresse de "multicast sollicité" pour le joindre. Ces adresses sont utilisées par les protocoles de détection d'adresse dupliquée et de découverte de voisins, qui seront abordés ultérieurement.

Plusieurs équipements sur le lien peuvent avoir la même adresse de "multicast sollicité". Mais, dans la pratique, la probabilité de trouver sur le même lien physique deux équipements avec les trois derniers octets de l'identifiant d'interface identiques est très faible. Cela permet donc de limiter le nombre d'équipements qui traiteront la requête de sollicitation de voisins. Ces adresses permettent de ne plus utiliser la diffusion généralisée (adresse MAC ff:ff:ff:ff:ff:ff) qu'utilise le protocole ARP en IPv4. Pour une station donnée, une adresse de "multicast sollicité" peut regrouper plusieurs adresses IPv6, par exemple l'adresse lien-local et l'adresse "unicast globale" si cette dernière est construite à partir de l'identifiant d'interface dérivé de l'adresse MAC de la carte Ethernet.

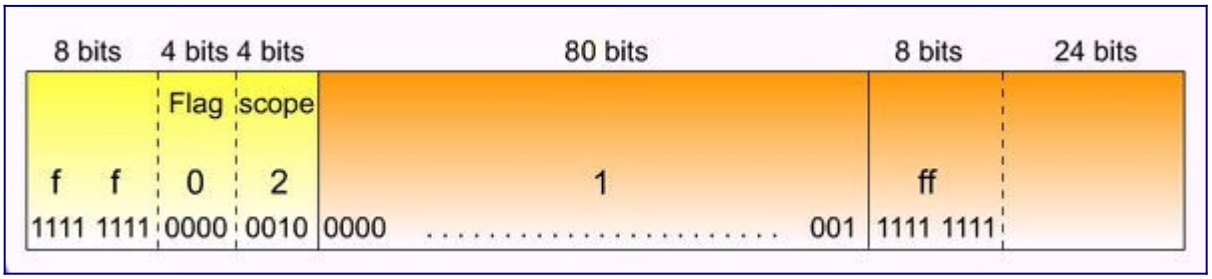

Figure 7 : Format de l'adresse "multicast sollicité".

Correspondance avec les adresses de multicast de niveau 2

Le RFC 3307 précise également la correspondance entre les adresses IPv6 multicast et les adresses de niveau 2. Sur un réseau de niveau 2 de type Ethernet, l'adresse MAC de multicast est déduite de l'adresse multicast IPv6 en concaténant les 32 derniers bits (4 octets) de l'adresse multicast IPv6 au préfixe MAC prédéfini 33-33. La figure 8 illustre le format multicast de niveau 2.

Par exemple, à l'adresse multicast IPv6 `ff0e:30:2001:660:3001:4002:ae45:2C56` correspondra l'adresse MAC `33-33-AE-45-2C-56`. La probabilité que deux adresses multicast IPv6 utilisées sur un même lien correspondent à la même adresse MAC existe mais est très faible et les conséquences minimes. Restreindre le champ `group-ID` à 32 bits a toutefois un intérêt car cela apporte une homogénéité entre les différents types d'adresses décrits précédemment. En effet, dans le cas des adresses dérivées d'un préfixe unicast, ce champ a une longueur de 32 bits.

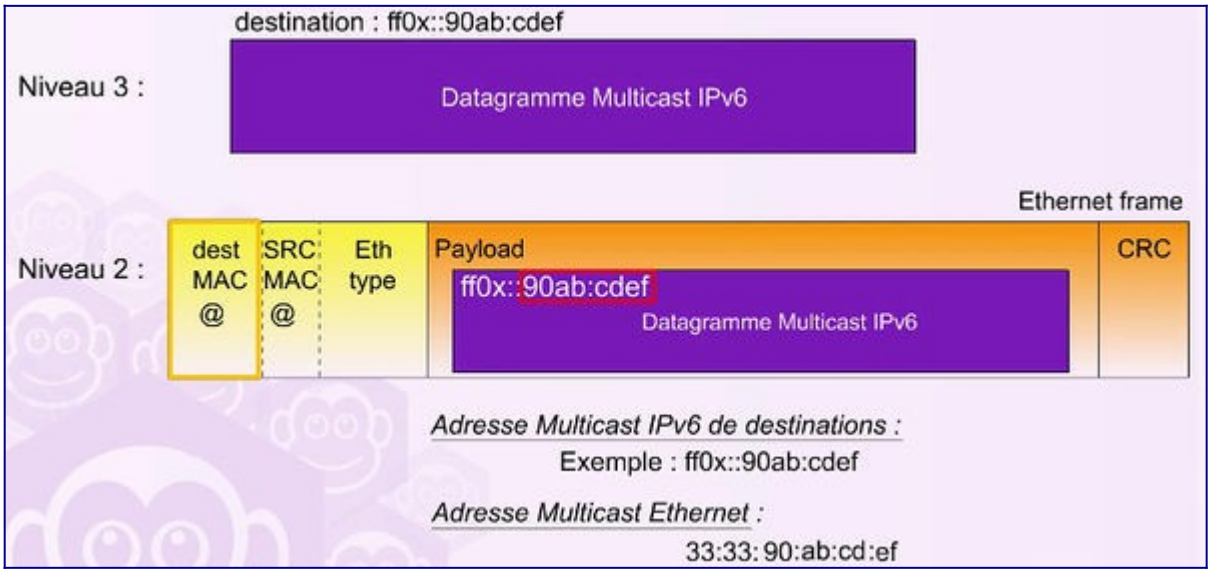

Figure 8 : Correspondance avec l'adresse multicast de niveau liaison.

Récapitulatif des types d'adresses multicast

Le tableau suivant récapitule les préfixes associés aux différents types d'adresses multicast décrit précédemment.

Préfixe	Usage
`ff0x::/16`	Adresses IPv6 multicast permanentes ;
`ff1x::/16`	Adresses IPv6 multicast temporaires générales ;
`ff3x::/16`	Adresses multicast dérivées d'un préfixe unicast (temporaires) ;
`ff3x::/96`	Adresses SSM (temporaires) ;
`ff7x::/16`	Adresses IPv6 multicast "Embedded-RP" (temporaires) ;
`ff02::1:ff00:0/104`	Adresses de "multicast sollicité" (préfixe prédéfini, portée limitée au lien).

(**x** : une des valeurs valides de la portée (*scope*))

Conclusion

Le fonctionnement du multicast en IPv6 reprend les principes énoncés pour IPv4. Nous venons de voir, dans cette activité, comment sont formatées les adresses IPv6 multicast. Nous vous invitons à approfondir l'exploration des fonctions multicast en consultant dans les références bibliographiques citées ci-après.

Références bibliographiques

1. ↥ Handley, M., Crowcroft, J., Internet Protocol Journal, Volume 2, No. 4, December 1999.

Internet Multicast Today
2. ↑ Cisco (2002). White paper. IP Multicast Technology Overview White paper Cisco.
3. ↑ Wikipedia. Le multicast IPv6
4. ↑ IANA IPv6 Multicast Address Space Registry

Pour aller plus loin

RFC et leur analyse par S. Bortzmeyer :

- RFC 2375 IPv6 Multicast Address Assignments
- RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
- RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3569 An Overview of Source-Specific Multicast (SSM)
- RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address
- RFC 4291 IP Version 6 Addressing Architecture Analyse
- RFC 4489 A Method for Generating Link-Scoped IPv6 Multicast Addresses
- RFC 7371 Updates to the IPv6 Multicast Addressing Architecture
- RFC 7346 IPv6 Multicast Address Scopes

Activité 14 : Plan d'adressage IPv6 unicast

Introduction

Lors de l'activité précédente, nous avons vu que les adresses IP unicast sont construites en combinant 2 éléments (voir la figure 1). Le premier élément vise à localiser le réseau dans l'Internet. Il sert à l'acheminement des paquets à travers l'Internet ou à travers l'interconnexion pour les infrastructures privatives. Le second élément identifie l'interface au sein de son réseau. Il sert à la remise directe du paquet à l'interface de destination sur le dernier saut de l'acheminement. Dans cette activité, nous nous intéressons à la construction de ces adresses unicast. Pour la partie préfixe de réseau, il s'agit de définir un plan d'adressage. Ce plan d'adressage est organisé de manière hiérarchique afin de permettre la délégation pour une gestion décentralisée mais aussi rendre les préfixes agrégables. L'objectif, dans ce dernier cas, est de constituer des tables de routage les plus concises possibles. Pour IPv6, vu la taille de l'espace d'adressage, cette caractéristique d'agrégation est essentielle. Dans cette activité, nous allons indiquer les différentes façons de numéroter les réseaux. Pour la partie identifiant d'interface, l'objectif est de définir un identifiant, si possible automatiquement, qui soit unique au sein du lien. Nous allons étudier les différentes techniques de constructions de ces identifiants. Mais avant, nous allons rappeler une caractéristique d'IPv6 dans l'utilisation des adresses unicast, à savoir la possibilité d'avoir plusieurs adresses unicast allouées à une interface de communication. Ces adresses multiples peuvent être utilisées simultanément ou l'une après l'autre. Un mécanisme de vieillissement est donc nécessaire pour limiter la validité d'une adresse.

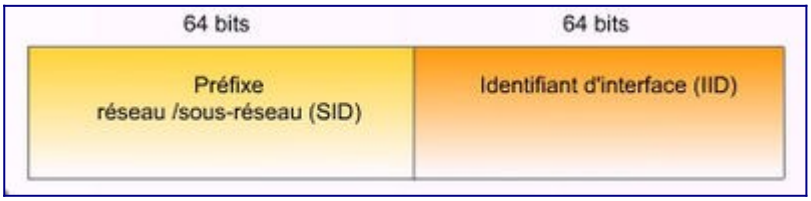

Figure 1 : Hiérarchisation de l'adresse unicast en deux parties logiques.

Enfin, pour conclure cette introduction, signalons que les conseils donnés par RIPE NCC sont précieux pour toutes personnes amenées à concevoir un plan d'adressage[1]. L'IETF a également édité un recueil de conseils pour le déploiement d'un réseau IPv6 par le RFC 7381.

Adressage multiple des interfaces

En IPv6, les interfaces de communication des nœuds disposent simultanément de plusieurs adresses. En effet, une interface dispose au moins d'une adresse purement locale sur son lien local (l'adresse lien-local). Celle-ci est automatiquement affectée à l'interface lors de la phase d'activation de cette dernière par le système d'exploitation. Selon la nature du lien de rattachement (liaison point à point, domaine de diffusion ethernet filaire ou wifi...), l'interface peut également disposer d'une ou plusieurs adresses routables soit localement (cas des adresses ULA), soit globalement (cas des adresses publiques : GUA). Ces adresses unicast routables sont constituées en associant le préfixe réseau associé au lien à l'identifiant d'interface. L'affectation de ces adresses routables peut être fait soit par l'administrateur

système de la machine, soit par le réseau en s'appuyant sur les mécanismes d'auto-configuration "avec" ou "sans état", comme nous le verrons dans une séquence ultérieure. La figure 2 illustre l'adressage multiple d'une interface de communication pour un nœud.

Figure 2 : Adressage multiple d'une interface de communication.

Nous savons, depuis l'activité "qu'est ce qu'une adresse IP ?", que les adresses IP ne sont pas permanentes. L'adresse IP a une durée de vie régie par des états. Ces états sont : provisoire, préféré, déprécié et invalide. Aussi, il faut comprendre qu'une adresse IP n'est allouée que temporairement à une interface. Il faut voir l'allocation comme un bail de location. Pour continuer d'utiliser une adresse IP, à l'expiration du bail, il faut procéder au renouvellement du bail. Ainsi, le système d'exploitation a en charge de renouveler périodiquement l'allocation d'une adresse IP en cours d'utilisation. Autrement, l'adresse passe dans l'état déprécié afin de rendre inutilisable cette adresse pour les nouvelles connexions et permettre de terminer les sessions et les connexions existantes. Il faut alors, dans un même temps, une nouvelle adresse valide pour les nouvelles connexions ou sessions applicatives. L'idée que les adresses IP sont allouées temporairement trouve sa motivation de rendre la renumérotation d'un réseau facile. La renumérotation d'un réseau consiste à remplacer un préfixe réseau par un autre. L'opération de renumérotation peut s'avérer nécessaire lorsque l'organisation change de fournisseur d'accès à Internet ou que le plan d'adressage est devenu obsolète. Il n'en reste pas moins que malgré les facilités qu'offrent IPv6, la renumérotation d'un réseau reste une opération périlleuse [RFC 5887].

Nécessité d'organiser un plan d'adressage

L'espace d'adressage IPv6 est « astronomiquement » grand. Il s'ensuit que le plan d'adressage unicast global adopté aujourd'hui est organisé hiérarchiquement. À l'instar du réseau téléphonique historique où les appels sont routés en fonction d'un préfixe national (exemple le +33 pour les appels vers la France), l'Internet est bâti selon une organisation hiérarchique. Cependant, cette hiérarchie n'est pas d'ordre géographique mais plutôt administrative et organisée en « régions » (Amérique du nord, Asie Pacifique, Europe,...). Chaque région est gérée par un registre Internet régional (*Regional Internet Registry* ou RIR). Cette organisation se retrouve au moment de l'acheminement des datagrammes dans l'Internet. Les opérateurs du cœur de l'Internet routent (aiguillent) les datagrammes selon les préfixes les plus courts. Les RIR leur attribuent des préfixes courts, car le rôle de ces opérateurs internationaux est d'acheminer les datagrammes vers les grandes zones régionales de l'Internet. Ces opérateurs délèguent ensuite à leur clients, registres locaux (LIR) ou opérateurs, des préfixes un peu plus

longs, afin qu'eux même puissent déléguer des préfixes à leurs clients ou organisations utilisatrices pour acheminer les datagrammes vers leurs propres réseaux. Ainsi, un utilisateur final (organisation, entreprise ou particulier) se verra déléguer par son fournisseur d'accès à Internet (FAI) un préfixe d'une longueur comprise, en général, entre 48 et 64 bits. La zone de l'adresse, comprise entre la longueur du préfixe alloué par l'opérateur et la limite du /64 des adresses unicast est parfois qualifiée de SID (*Subnet ID*). En effet, elle permet à l'administrateur d'adresser entre un unique réseau (cas où le client a obtenu un préfixe /64 de son FAI) et 65536 réseaux (cas où le client a obtenu délégation administrative de son FAI sur un préfixe /48 : il dispose alors de 16 bits (entre 48 et 64) pour numéroter 2 puissance 16 soit 65536 réseaux). C'est cet espace d'adressage dont l'administrateur réseau a la responsabilité. Il s'agit pour lui d'organiser cet espace pour déployer efficacement les réseaux de son organisation. Nous allons maintenant présenter différents modes d'organisation possibles en nous appuyant sur le RFC 5375.

Politique d'assignation des adresses

Les spécifications primitives d'assignation des adresses [RFC 3177] aux utilisateurs finaux recommandaient d'allouer :

- /48 (65536 sous-réseaux) dans le cas général,
- /64 (un sous-réseau unique) lorsqu'un et un seul réseau physique était nécessaire,
- /128 (adresse unique) lorsqu'il était absolument connu qu'un et un seul équipement était connecté.

Le RFC 6177, également connu sous BCP157 (*Best Current Practice*), est venu remettre en cause les certitudes initiales et le « /48 pour tout le monde » n'est plus la recommandation officielle. La taille du préfixe est maintenant laissée à la discrétion du fournisseur avec la recommandation « floue » d'allouer un bloc d'adresses adapté aux besoins de l'utilisateur en évitant l'allocation d'un réseau unique. Ainsi, si un /48 est adapté pour un réseau de campus, il est clairement surdimensionné dans le cadre d'un usage domestique. Inversement, le réseau unique en /64 est notablement insuffisant ; les besoins actuels et futurs de la plupart des foyers nécessiteront sans doute quelques réseaux cloisonnés en fonction des usages : réseau général (accès internet, les réseaux sociaux, le multimédia...), réseau domotique (lave-linge, sèche-linge, réfrigérateur...), réseau de commande périmétrique (volets, alarme, chauffage, aquarium...), sans parler des promesses médiatiques de l'Internet des objets (IoT *Internet of Things*). Pour les utilisateurs dits « grand public » ou les sites de taille modeste, un préfixe /56 ou /60 semble donc plus approprié.

Préfixes de sous-réseaux (SID Subnet IDentifier)

Les sous-réseaux IPv6 doivent s'aligner sur les préfixes de longueur /64. Des tailles supérieures sont possibles, mais ne sont pas sans poser problème pour les mécanismes de contrôle tels que l'auto-configuration des adresses, couramment utilisée, et qui présupposent des préfixes des sous-réseaux alignés sur 64 bits. Ces mécanismes d'auto-configuration seront abordés dans une séquence ultérieure.

Ces préfixes de 64 bits sont construits à partir du préfixe global permettant le routage des paquets vers le réseau du site regroupant ces sous-réseaux. Le préfixe global est celui utilisé dans les tables de routage de l'opérateur connectant le site à Internet. À ce préfixe global est ajouté la valeur identifiant le sous-réseau à l'intérieur du réseau du site. Cette valeur est définie sur le nombre de bits restant pour définir un préfixe unique de 64 bits. Ce préfixe sera utilisé dans les tables de routage internes au réseau du site. La figure 3 décrit cette hiérarchie de la partie préfixe de l'adresse.

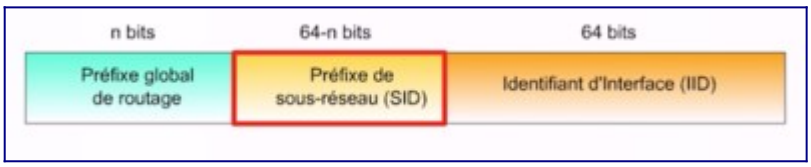

Figure 3 : Hiérarchisation de la partie préfixe.

Représentation des subdivisions

Dans la suite de cette activité, nous raisonnerons sur la base d'un préfixe de 48 bits (espace SID de 16 bits). Les exemples décrits sur la base d'adresses documentaires pourront ainsi illustrer aussi bien un contexte de réseaux publics (un préfixe /48 unicast global) qu'un réseau privatif (préfixe /48 d'adresse locale unique ULA). Cependant, les règles d'ingénierie présentées pourront également se décliner de manière plus limitée sur des préfixes plus longs /56 ou /60 avec un espace SID réduit à 8 ou 4 bits.

Nous supposons que le préfixe pour notre activité est `2001:db8:cafe::/48`. Le préfixe est obtenu :

- soit par allocation de notre fournisseur d'accès dans le cadre d'un adressage unicast global routable sur l'Internet public,
- soit par algorithme conforme RFC 4193 dans la cadre d'un adressage privatif (ULA Unique unicast Local Address).

Nous disposons donc d'une zone SID de 16 bits permettant de distinguer 65536 sous-réseaux possibles en préfixes de 64 bits (de `2001:db8:cafe::/64` à `2001:db8:cafe:ffff::/64`).

Convention de notation binaire du champ SID

Dans cette présentation, nous adoptons les conventions de notation suivantes pour les illustrations et exemples : Comme les 48 premiers bits sont administrativement fixés et que les 64 bits de poids faible sont réservés pour l'identification de l'interface, chaque référence de sous-réseau sera portée par les bits 48 à 63 (L'IETF numérote les bits en démarrant de zéro de la gauche (most significant : poids fort) à la droite (least significant : poids faible).

Exemple :

`2001:db8:cafe:{LLLLTTTTBBBBBBBB}::/64`

ou

`2001:db8:cafe:ltbb::/64`

- Chaque lettre majuscule encadrée par '{' et '}' représente 1 bit du champ SID. 4 bits successifs représentent un quartet également appelé « nibble » ;

  *(Un **nibble** (ou plus rarement **nybble**) est, en informatique, un agrégat de 4 bits, soit un demi-octet. On trouve aussi les termes francisés **semioctet** ou **quartet** , source wikipédia https://fr.wikipedia.org/wiki/Nibble)*. Un quartet peut prendre une valeur entre 0 et 15 et peut se représenter par un chiffre hexadécimal (0..9, a..f) (cf. vademecum de notation hexadécimale) ;
- Les chiffres et lettres minuscules ['a'..'f'] représentent la valeur hexadécimale d'un quartet ;
- Dans cette présentation, nous subdivisons les 16 bits du SID en groupes distingués de la manière suivante :
  - B : bit non défini et assignable ;
  - L : bit assigné à l'identification de la localisation du sous-réseau ;
  - T : bit assigné à l'identification du type de sous-réseau.

Ainsi, l'exemple précédent où les 16 bits SID sont positionnés à la valeur `{LLLLTTTTBBBBBBBB}` produira des préfixes IPv6 du type `2001:db8:ltbb::/64`. Inversement, si l'on choisit de positionner les bits de "type de sous-réseau" sur le quartet de poids fort et les bits de localisation sur le quartet de poids faible du 1er octet SID de cette manière `{TTTTLLLLBBBBBBBB}`, cela produira un préfixe de type `2001:db8:tlbb::/64`.

Différentes stratégies d'allocation des valeurs de SID sont présentées en annexe. Un administrateur peut les mettre en pratique pour définir un plan d'adressage pour son réseau.

Cas particulier des liaisons point à point

Les liaisons point à point, qu'elles soient concrètement louées auprès du service idoine d'un opérateur (liaison spécialisée, fibre noire...) pour assurer l'interconnexion de deux sites géographiquement distants, ou qu'elles soient logiquement établies sous forme de tunnels (IP dans IP, VPN MPLS, tunnel IPSec…) constituent un cas particulier. Dans le cas général, on peut allouer un préfixe /64 à chacune des liaisons. Cependant, sur des réseaux maillés où le nombre de liaisons point à point est quelconque, attribuer un /64 à chacune de ces liaisons n'est pas efficace. La caractéristique d'une liaison point à point est de relier uniquement une interface à chacune de ses extrémités, ne nécessitant, de fait, que deux identifiants distincts. De plus, ces liaisons sont administrées et ne sont, en général, pas tributaires d'un mécanisme d'auto-configuration. Aussi, attribuer un /64 offrant la possibilité d'adresser 2 puissance 64 interfaces à un support limité à deux, et uniquement deux interfaces, conduit à la perte de ((2 puissance 64) - 2) adresses qui resteront non attribuées. L'utilisation d'un /64 sur une liaison point à point peut conduire à des problèmes de sécurité (RFC 6164): soit sous la forme d'aller-retours de datagrammes sur cette liaison (syndrome de la balle de ping-pong) entraînant une congestion du support, ou soit sous la forme de déni de service des routeurs connectés au lien

au travers d'une saturation des caches de découverte des voisins. À défaut d'un /64, quel est le préfixe approprié pour ce type de liaison ?

- /127 serait possible dans la mesure où IPv6 n'a pas d'adresse de diffusion (identifiant de *host* tout à 1 dans le cas d'IPv4). Cependant, l'adresse tout à zéro de chaque sous-réseau est réservée comme l'adresse anycast des routeurs (*all routers anycast address*), ce qui signifie que la plupart des routeurs sont susceptibles de recevoir des datagrammes de service sur cette adresse.
- /126 évite le problème de l'adresse anycast tout à zéro. Cependant, les 128 adresses hautes de chaque sous-réseau sont également réservées pour diverses adresses d'anycast (RFC 2526) ; bien que, dans la pratique, cela ne semble pas poser de problème.
- /120 permet de s'affranchir des adresses anycast réservées.
- /112 permet de s'affranchir des adresses anycast réservées et a, en plus, l'avantage d'être facilement lisible par les opérateurs humains car aligné sur le mot de 16 bits final (celui affiché après le dernier séparateur *:*, cf. activité 12 « Notation d'une adresse IPv6 »).

Le RFC 6164 recommande l'utilisation d'un préfixe de longueur /127 pour IPv6, ne permettant ainsi que deux adresses IP.

Identification locale : l'IID (Interface IDentifier)

Les identifiants d'interfaces des adresses unicast sont utilisés pour identifier de manière unique les interfaces des équipements sur un lien ou un domaine de diffusion de niveau 2 (VLAN). Ils doivent absolument être uniques pour le domaine couvert par un sous-réseau. Toutefois, l'unicité d'un identifiant d'interface peut être de portée beaucoup plus large, voire globale, à l'image des adresses MAC dont l'unicité est mondiale. Dans certains cas, l'identifiant d'interface sera dérivé directement de l'adresse de niveau liaison de données (adresse MAC de la carte Ethernet par exemple).

Pour les adresses unicast, à l'exception des adresses non spécifiées ou de l'adresse de bouclage (*loopback*) (celles commençant par 000), l'identifiant d'interface doit avoir une longueur de 64 bits. La taille de 64 bits permet d'approcher une probabilité de conflit quasi nulle.

Si, initialement, pour des raisons d'auto-configuration, l'identifiant d'interface devait nécessairement être dérivé de l'adresse de niveau 2 (adresse matérielle), c'est de moins en moins le cas. Il existe plusieurs méthodes pour construire cette valeur de 64 bits [RFC 8981] :

- manuelle,
- basée sur l'adresse de niveau 2 de l'interface [RFC 4291],
- temporaire aléatoire [RFC 8981],
- stable opaque [RFC 7217]
- cryptographique [RFC 3972].

Identifiant manuel

Pour les serveurs les plus utilisés, il est préférable d'assigner manuellement des adresses aux interfaces car, dans ce cas, l'adresse IPv6 est facilement mémorisable et le serveur peut être accessible, même si le DNS n'est pas actif.

Nota : Le résolveur DNS est le cas le plus emblématique. Chaque machine sur le réseau doit être configurée avec son client DNS pointant vers l'adresse du serveur DNS. Si celui-ci a un identifiant d'interface basé sur l'adresse de niveau 2, en cas de changement de la carte réseau sur le serveur DNS, l'ensemble des machines du domaine devraient être reconfigurées. Si l'on ne souhaite pas utiliser de protocole de configuration automatique tel DHCPv6, il est préférable d'attribuer au serveur DNS une valeur manuelle d'identifiant d'interface. Cette valeur statique sera stable dans le temps et pourra être utilisée pour référencer le résolveur DNS sur la configuration de l'ensemble des machines du réseau.

Il existe plusieurs techniques plus ou moins mnémotechniques :

- Incrémenter l'identifiant d'interface à chaque nouveau serveur créé.

```
2001:db8:1234:1::1

2001:db8:1234:1::2
```

- Reprendre le dernier octet de l'adresse IPv4 comme identifiant d'interface. Par exemple, si un serveur a comme adresse IPv4 192.0.2.123, son adresse IPv6 pourra être :

```
2001:db8:1234:1::7B
```

ou plus simplement

```
2001:db8:1234:1::123
```

- Reprendre l'adresse IPv4 comme identifiant d'interface, bien que cela ait l'inconvénient de conduire à des adresses plus longues à saisir :

```
2001:db8:1234:1::192.0.2.123
```

Identifiant dérivé de l'adresse matérielle de l'interface

L'avantage d'utiliser une adresse de niveau 2 pour construire un identifiant d'interface est que l'unicité de cette valeur est presque toujours assurée. En plus, cette valeur est stable tant que la carte réseau de la machine n'est pas changée. Par contre, ces valeurs sont difficilement mémorisables.

Les adresses lien-local sont en général construites en utilisant ce type d'identifiant. Par contre, pour les adresses globales, il est conseillé de ne les utiliser que pour les machines clientes et de préférer les identifiants d'interfaces manuels pour les serveurs.

Ces identifiants d'interfaces étant stables dans le temps, à chaque fois qu'un individu change de réseau, il change de préfixe, mais garde le même identifiant d'interface. Ce dernier pourrait donc servir à tracer les déplacements d'un individu[2]. Ce sujet de traçabilité et de respect de la vie privée a fait l'objet d'une prise de conscience collective suite à une actualité récente (affaire

Snowden, surveillance de masse par les états, écoute de la NSA...). Mais, la traçabilité par l'identifiant d'interface n'en est qu'un des éléments car les cookies mis en place par les serveurs web ou les recoupements d'infos personnelles déposées sur les réseaux sociaux sont bien plus efficaces ; mais ils ne s'agit plus d'un problème réseau. Autre désavantage : comme les adresses MAC contiennent l'identification du matériel, il est possible d'indiquer à l'extérieur du réseau quel type de matériel est utilisé et donner des indications.

Si ces inconvénients sont jugés importants par l'entreprise, l'identifiant d'interface pour les adresses globales peut être généré aléatoirement.

Identificateur EUI-64

L'IEEE a défini un identificateur global à 64 bits (format EUI-64) pour les réseaux IEEE 1394 (Firewire) ou IEEE 802.15.4 (réseaux de capteurs) qui vise une utilisation dans le domaine de la domotique. L'IEEE décrit les règles qui permettent de passer d'un identifiant MAC codé sur 48 bits à un EUI-64.

Si une machine ou une interface possède un identificateur global IEEE EUI-64, celui-ci a la structure montrée par la figure 7. Les 24 premiers bits de l'EUI-64, comme pour les adresses MAC IEEE 802.3, identifient le constructeur. Les 40 autres bits identifient le numéro de série (les adresses MAC IEEE 802 n'en utilisaient que 24). Les 2 bits, u (septième bit du premier octet), et g (huitième bit du premier octet) ont une signification spéciale :

- u (Universel) vaut 0 si l'identifiant EUI-64 est universel ;
- g (Groupe) indique si l'adresse est individuelle (g = 0), c'est-à-dire désigne un seul équipement sur le réseau, ou de groupe (g = 1), par exemple une adresse de multicast.

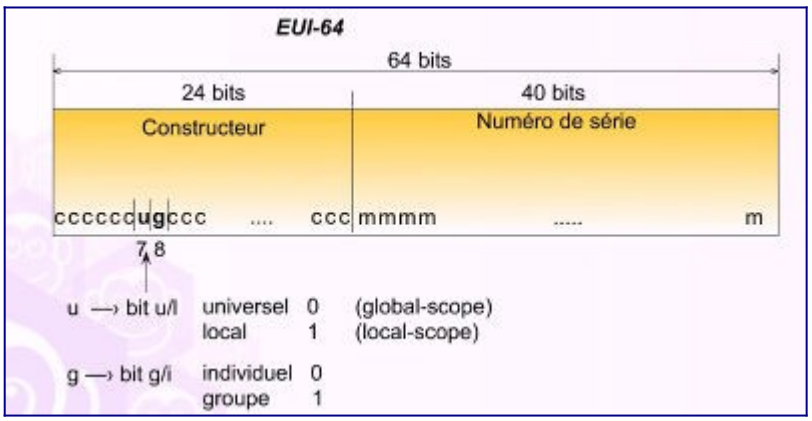

Figure 7 : Format de l'identificateur IEEE EUI-64.

Dans le cas d'IPv6, l'identifiant d'interface à 64 bits peut être dérivé de l'EUI-64 en inversant le bit u comme le montre la figure 8. En effet, pour la construction des adresses IPv6, on a préféré utiliser 1 pour marquer l'unicité mondiale. Cette inversion de la sémantique du bit permet de garder la valeur 0 pour une numérotation manuelle, autorisant à numéroter simplement les interfaces locales à partir de 1.

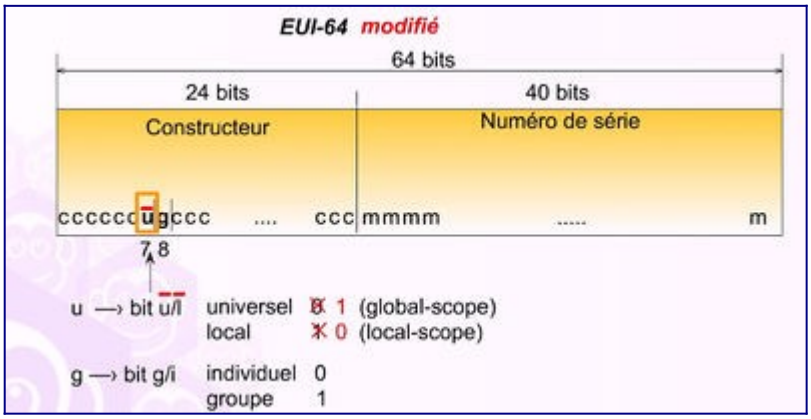

Figure 8 : Identifiant d'interface dérivé du format EUI-64.

Identificateur MAC-48

Si une interface possède une adresse MAC IEEE 802 à 48 bits universelle (cas des interfaces Ethernet ou Wi-Fi), l'adresse est tout d'abord convertie en EUI-64 par l'insertion de 16 bits à la valeur 0xfffe, puis le bit u est mis à 1 comme dans le cas précédent. La figure 9 illustre ce processus.

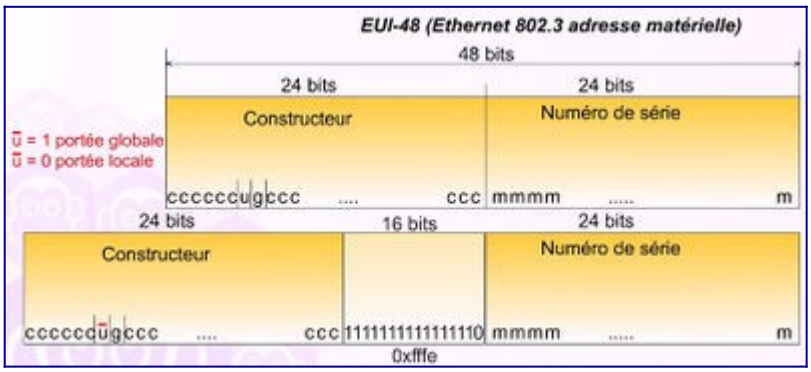

Figure 9 : Identifiant d'interface dérivé de l'adresse MAC (EUI-48).

Cas Particuliers

Si une interface ne possède aucune adresse, par exemple l'interface utilisée pour les liaisons PPP (*Point to Point Protocol*), et si la machine n'a pas d'identifiant EUI-64, il n'y a pas de méthode unique pour créer un identifiant d'interface. La méthode conseillée est d'utiliser l'identifiant d'une autre interface si c'est possible (cas d'une autre interface qui a une adresse MAC), ou une configuration manuelle, ou bien une génération aléatoire avec le bit u positionné à 0. S'il y a conflit (les deux extrémités ont choisi la même valeur), il sera détecté lors de l'initialisation de l'adresse lien-local de l'interface, et devra être résolu manuellement.

Opacité des identifiants d'interface

Les bits u et g n'ont de signification que pour les adresses de niveau MAC (adresse EUI-64 et EUI-48). Si, aux origines d'IPv6 (RFC 4291), le bit u conservait cette signification d'universalité, c'est qu'à l'époque l'identifiant d'interface dérivait majoritairement de l'adresse matérielle. C'est moins le cas aujourd'hui avec les IID temporaires aléatoires, voire cryptographiques (cf. paragraphes suivant). L'IETF a remis les choses au clair dans le RFC 7136 en précisant

maintenant que "les identifiants d'interface doivent être considérés comme opaques et il ne faut pas tirer de conclusion de la valeur de tel ou tel bit". La dérivation d'un IID à partir d'une adresse matérielle reste inchangée mais, inversement, si on ne sait pas comment a été généré l'IID, on ne peut rien déduire de la signification des deux bits de poids faible de l'octet de poids fort de l'IID. N'attachez donc pas plus d'importance à ces bits qu'ils n'en n'ont réellement aujourd'hui.

Valeur temporaire aléatoire

L'identifiant d'interface basé sur des adresses MAC, comme indiqué précédemment, pourrait poser des problèmes pour la vie privée. Il identifie fortement la machine d'un utilisateur qui, même s'il se déplace de réseau en réseau, garde ce même identifiant. Il serait alors possible de traquer un individu mobile utilisant un portable, chez lui, au bureau, lors de ses déplacements.

Pour couper court à toutes les menaces de boycott d'un protocole qui « menacerait la vie privée », l'IETF a validé d'autres méthodes de construction d'un identifiant d'interface comme celle reposant sur des tirages aléatoires [RFC 8981]. Un utilisateur particulièrement méfiant pourrait activer ces mécanismes. L'identifiant d'interface est soit choisi aléatoirement, soit construit par un algorithme de hachage, comme MD5, à partir des valeurs précédentes, soit tiré au hasard si l'équipement ne peut pas mémoriser d'information entre deux démarrages. Périodiquement, l'adresse est mise dans l'état « déprécié » et un nouvel identifiant d'interface est choisi. Les connexions déjà établies continuent d'utiliser l'ancienne valeur tandis que les nouvelles connexions utilisent la nouvelle adresse.

Cette solution a été adoptée par Microsoft. Dans Windows XP, l'interface possède deux adresses IPv6 globales comme on le voit dans la figure 10. La première a un identifiant d'interface dérivé de l'adresse MAC. Elle sert aux applications attendant des connexions sur la machine (*i.e.* les applications "serveur"). Cette adresse est stable et peut être publiée dans le DNS. La seconde possède un identifiant d'interface tiré aléatoirement. Elle est changée tous les jours ou à chaque redémarrage de la machine et sert aux applications clientes. Dans Windows 7, ce comportement est généralisé car l'identifiant d'interface de l'adresse permanente est également issu d'un tirage aléatoire. Cela permet d'éviter de donner la marque de la machine ou le type de carte contenu dans les premiers octets de l'identifiant d'interface. Elle est également présente, mais de manière optionnelle, sur les systèmes d'exploitation Linux, BSD et Mac OS.

Bien entendu, pour que ces mécanismes aient un sens, il faut que l'équipement ne s'enregistre pas sous un même nom dans un serveur DNS inverse, et que l'enregistrement de cookies dans un navigateur Web pour identifier l'utilisateur soit impossible.

En contre-partie, il est plus difficile à un administrateur réseau de filtrer les machines puisque celles-ci changent périodiquement d'adresses.

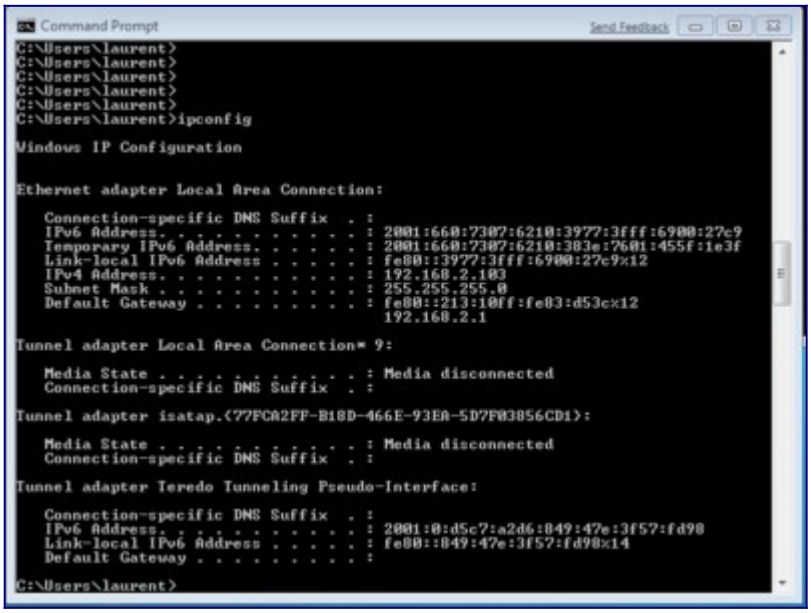

Figure 10 : Adresse IPv6 temporaire de MS-Windows.

Valeur stable opaque

L'identifiant d'interface dérivé de l'adresse matérielle pose le problème de la traçabilité des équipements nomades et de respect de la vie privée qui en découle. Cependant, il dispose de la propriété de stabilité (*on éteint la machine et on la rallume, on est sûr de retrouver la même adresse IPv6*) qui simplifie les tâches administratives (*Ainsi, lorsqu'on regarde le journal des connexions, on peut facilement retrouver la machine qu'on a repéré. Et créer des ACL est simple, puisque les adresses ne changent pas*). Le RFC 7217 propose une méthode de génération de l'IID opaque, ne révélant pas d'information relativement à la configuration matérielle, mais stable dans le temps. Le principe est de condenser (à l'aide d'une fonction de hachage telle que SHA-256 par exemple et de ne conserver que les 64 bits de poids faible) un secret (stocké dans une mémoire non volatile), un certain nombre de caractéristiques de la machine et le préfixe, de manière à avoir des identifiants stables, mais préservant quand même partiellement la vie privée de postes nomades : l'identifiant d'interface change quand la machine change de réseau, ne permettant plus de la suivre à la trace. Mais, si on reste sur le même réseau, l'adresse est stable. Le RFC 8064 a confirmé la prééminence de cette méthode sur la méthode dérivée de l'adresse MAC pour la procédure d'autoconfiguration sans état (*qui sera décrite dans la séquence 3*).

L'idée est que la machine aurait une ou plusieurs adresses temporaires, une ou plusieurs adresses stables et qu'on utiliserait l'adresse temporaire pour les connexions sortantes, et l'autre pour les entrantes. Cela fournit une bonne protection de la vie privée, mais au prix de quelques inconvénients. Comme rien n'est gratuit en ce bas monde, ces adresses compliquent la vie de l'administrateur réseaux : interpréter le trafic qu'on voit passer est moins simple (beaucoup de techniques de protection de la vie privée ont ce défaut).

Cryptographique

Si un identifiant aléatoire permet de rendre beaucoup plus anonyme la source du paquet, des

propositions sont faites à l'IETF pour lier l'identifiant d'interface à la clé publique de l'émetteur du paquet. Le RFC 3972 définit le principe de création de l'identifiant d'interface (CGA : *Cryptographic Generated Addresses*) à partir de la clé publique de la machine. Elles pourraient servir pour sécuriser les protocoles de découverte de voisins ou pour la gestion de la multi-domiciliation.

Conclusion

Une interface de communication en IPv6 peut avoir plusieurs adresses unicast. Les adresses IP sont allouées temporairement. On parle alors d'une durée de vie d'une adresse qui est en fait sa durée d'allocation. L'intérêt est de rendre la renumérotation, c'est-à-dire le changement d'adresse, rapide et automatique.

L'adresse unicast IPv6 est découpée en 2 parties. Une partie va servir à l'identification mais aussi à la localisation du réseau au sein de l'Internet. On parle de préfixe réseau. Nous avons étudié comment définir et organiser un plan d'adressage de manière hiérarchique afin de permettre la délégation pour une gestion décentralisée mais aussi rendre les préfixes agrégables, afin de constituer des tables de routage les plus concises possibles. Pour IPv6, vu la taille de l'espace d'adressage, cette caractéristique d'agrégation est essentielle. La seconde partie de l'adresse sert à identifier une interface au sein d'un lien. Nous avons présenté les différents modes de construction des identifiants d'interfaces.

Références bibliographiques

1. ↑ RIPE NCC (2013), publiée sous licence CC-BY par Surfnet (www.surfnet.nl) *Preparing an IPv6 address plan*
2. ↑ Internet society. (2014) Deploy 360 programm IPv6 Privacy Addresses Provide Protection Against Surveillance And Tracking

Pour aller plus loin

RFC et leur analyse par S. Bortzmeyer :

- RFC 3972 Cryptographically Generated Addresses (CGA)Analyse
- RFC 4291 IP Version 6 Addressing Architecture Analyse
- RFC 5375 IPv6 Unicast Address Assignment Considerations Analyse
- RFC 5887 Renumbering Still Needs Work Analyse
- RFC 6164 Using 127-Bit IPv6 Prefixes on Inter-Router Links :;m=Analyse
- RFC 6177 IPv6 Address Assignment to End Sites Analyse
- RFC 7136 Significance of IPv6 Interface Identifiers Analyse
- RFC 7217 A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) Analyse
- RFC 7381 Enterprise IPv6 Deployment Guidelines Analyse
- RFC 7934 Host address availability recommendations Analyse
- RFC 8064 Recommendation on Stable IPv6 Interface Identifiers Analyse

- RFC 8065 Privacy Considerations for IPv6 Adaptation-Layer Mechanisms Analyse
- RFC 8981 Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6 Analyse

Annexe : Différentes stratégies pour la définition des sous-réseaux (SID)

Lorsqu'un administrateur a pour tâche de déployer IPv6 sur son réseau, une des étapes importantes est la définition du plan d'adressage. Ce plan définit l'ensemble des adresses utilisées sur chacun des réseaux du site concerné. En IPv6, chaque réseau se voit attribuer un préfixe nécessairement de largeur 64 bits (/64). L'administrateur connaissant le préfixe assigné à son site, communément de largeur 48 bits, il lui reste à définir les 16 bits restants pour identifier chacun de ces réseaux. Cette valeur est appelé identifiant de sous-réseau ou SID.

Réseau à plat

Les petites entités sans structure organisationnelle bien définie peuvent éventuellement fonctionner sans plan d'adressage structuré. Cependant, si l'infrastructure de niveau liaison est cloisonnée en domaines de diffusion distincts (VLAN), il faudra affecter au moins un identifiant de sous-réseau par domaine. L'attribution de ces identifiants de sous-réseaux pourra être simple, en numérotant éventuellement séquentiellement.

En l'absence de structuration du plan d'adressage, ce type de réseau ne passe pas à l'échelle. Si le nombre de sous-réseaux est amené à croître, l'administration et le contrôle de l'infrastructure deviennent rapidement problématiques. Il y a également nécessité de conserver dans une table les différentes affectations pour localiser le segment réseau ou la machine à l'origine d'un problème ou d'un dysfonctionnement puisque les adresses sont peu signifiantes.

Correspondance directe entre les identifiants IPv4 et IPv6

Pour les organisations ayant déjà structuré une infrastructure réseau sous le protocole IPv4, et sur laquelle on souhaite faire cohabiter les deux versions du protocole, il est possible d'adopter une stratégie de correspondance des identifiants de sous-réseau IPv4 et de sous-réseau IPv6. Deux cas peuvent être évalués :

Correspondance directe entre les sous-réseaux IPv4 et IPv6

Si les réseaux IPv4 sont structurés uniquement en sous-réseaux de préfixe /24 (exemple les réseaux privatifs du RFC 1918, un réseau de classe C `192.168.0.0/24` à `192.168.255.0/24` ou que l'on a « subnetté » en /24 le réseau de classe A `10.0.0.0` ou l'un des 16 classe B `172.16.0.0` à `172.31.0.0`), une correspondance directe entre l'identifiant de sous-réseau IPv4 peut être envisagée avec l'identifiant SID d'IPv6 par transcription directe.

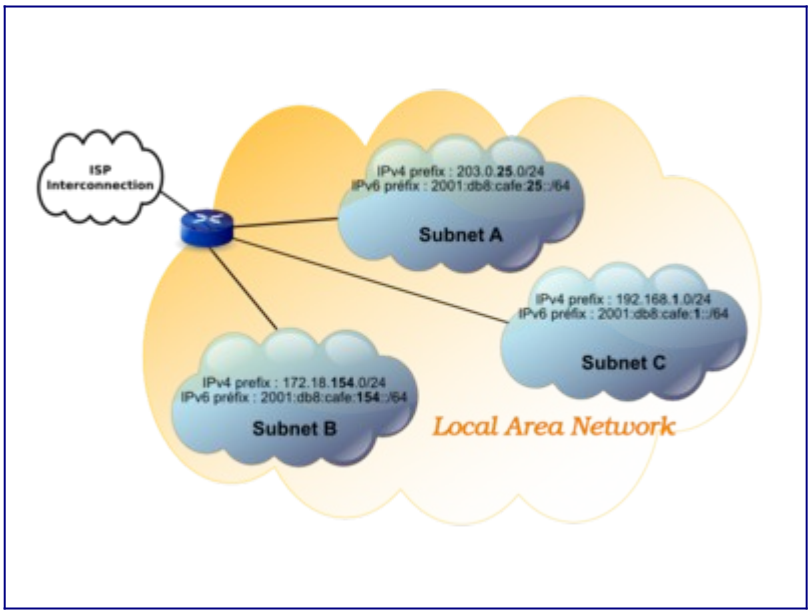

Figure 3 : Exemple de réseau.

Dans l'exemple du plan d'adressage de la figure 3, le lien direct entre les sous-réseaux IPv4 et les sous-réseaux IPv6 est directement visible. Pour les équipements d'infrastructure disposant d'une adresse fixe (routeur, serveurs applicatifs...) on peut également transposer l'identifiant d'hôte (4e octet d'adresse IPv4 d'un /24) en identifiant d'interface de l'adresse IPv6. Ainsi, par exemple, le serveur web d'adresse IPv4 `192.168.1.123` peut être adressé `2001:db8:cafe:1::123` en IPv6.

Cependant, cette stratégie ne peut s'envisager que si les sous-réseaux IPv4 sont alignés sur 24 bits (/24). En effet, des sous-réseaux IPv4 de taille plus étendue (préfixe < /24) ou plus réduite (préfixe > /24) ne peuvent s'insérer dans le champ SID de 16 bits d'un préfixe IPv6 en /64 (le débordement au-delà du /64 posant des problèmes pour l'auto-configuration). Ainsi :

- un préfixe IPv4 /28, par exemple les hôtes `172.16.5.14/28` et `172.16.5.18/28` sont dans des sous-réseaux IPv4 distincts : le sous-réseau `172.16.5.0/28` pour le premier et le sous-réseau `172.16.5.16/28` pour le second. Alors que la transposition simple en IPv6 va les placer dans le même sous-réseau : les hôtes `2001:db8:cafe:5::14/64` et `2001:db8:cafe:5::18/64` sont tous les deux dans le sous-réseau `2001:db8:cafe:5::/64`.
- Un préfixe IPv4 /23, par exemple les hôtes `10.0.8.250/23` et `10.0.9.5/23` sont tous les deux dans le même sous-réseau IPv4. Alors que la transposition simple les placera dans des sous-réseaux IPv6 distincts : `2001:db8:cafe:8::250/64` et `2001:db8:cafe:9::5/64`

On notera également que la transposition directe des identifiants décimaux des sous-réseaux IPv4 dans le champ SID hexadécimal du sous-réseau IPv6, si elle facilite la correspondance de lecture pour l'administrateur humain, n'est en revanche pas optimale pour les tables de routage des sous-réseaux IPv6. Ainsi, le sous-réseau IPv4 `10.0.23.0/24` est sélectionné (filtré / masqué) sur un octet de valeur binaire 0001 0111, alors qu'il sera sélectionné par le SID 0x0023

hexadécimal (0000 0000 0010 0011)

Correspondance directe entre les adresses IPv4 et IPv6

Si le préfixe de sous-réseau IPv4 n'est pas aligné sur un /24, il sera impossible de maintenir une relation directe entre les sous-réseaux IPv4 et IPv6. Cependant, dans ce cas, il peut être envisagé de maintenir une correspondance d'adresse en embarquant la totalité de l'adresse IPv4 dans l'identifiant d'interface de l'adresse IPv6 et en gérant le SID indépendamment du sous-réseau IPv4. Par exemple, la machine d'adresse IPv4 `192.168.1.234` pourrait être adressée en IPv6 `2001:db8:cafe:deca::192.168.1.234`. En effet, pour les adresses IPv6 embarquant une adresse IPv4, si celle-ci occupe les 32 bits de poids faible de l'adresse IPv6 (la partie basse de l'identifiant d'interface), il est autorisé de continuer à la noter en notation décimale pointée. Cependant, si cette commodité facilite la saisie de la configuration d'un système, celui-ci l'affichera sous la forme canonique `2001:db8:cafe:deca::c0a8:1ea`, notamment dans les journaux et log diverses. c0a801ea étant la conversion hexadécimale des 32 bits de l'adresse IPv4 écrite `192.168.1.234` en notation décimale pointée, la correspondance de lecture devient tout de suite moins évidente.

Plan d'adressage structuré

Lorsque l'on définit un plan d'adressage tel que sur la figure 4, il faut décider quelle structure doit être utilisée pour assigner les adresses aux réseaux de l'organisation. Plusieurs stratégies peuvent être envisagées. En nous appuyant sur l'exemple d'architecture suivante, nous allons présenter différents plans possibles.

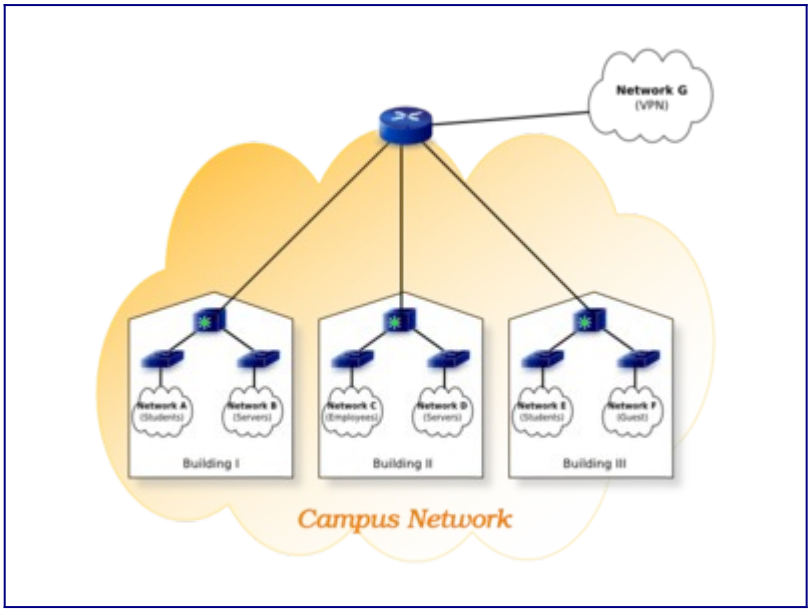

Figure 4 : Plan d'adressage structuré

Structuration basique du plan d'adressage

Nous pouvons, par exemple, assigner les adresses des équipements par type d'usage ou par localisation, voire une combinaison des deux. Ainsi, nous pouvons choisir d'adresser d'abord

par localisation, puis par type. Une fois les sous-réseaux définis, il restera les bits de poids faible qui pourront être utilisés pour d'autres usages, *(selon la convention de notation définie précédemment le préfixe se représente de la manière suivante) :*

```
2001:db8:cafe:{LLLLTTTTBBBBBBBB}::/64
```

Dans cet exemple, 4 bits sont assignés pour la localisation {L}. Les 4 bits suivants sont assignés pour le type d'usage {T}. Il reste 8 bits {B} pour d'autres affectations. Ainsi, ce plan d'adressage permet d'adresser une infrastructure qui peut être étendue sur 16 (4 bits) localisations, chacune pouvant déployer 16 (4 bits) types de réseaux. On dispose encore de 8 bits restants permettant éventuellement 256 sous-réseaux différents pour chaque localisation et chaque type.

Routeur vs firewall : localisation ou type d'usage d'abord ?

Nous devons, dans un premier temps, décider quelle affectation nous souhaitons privilégier : localisation d'abord puis type (tels que public/DMZ, employés, étudiants, invités, switchs, routeurs, serveurs, administration, comptabilité, production, etc.) ou inversement : type avant la localisation. La figure 5 illustre ces besoins.

Localisation d'abord

Quand la structuration se fait d'abord sur la localisation, chaque campus, bâtiment, département, est administrativement identifié par une référence. Cela permet d'optimiser les tables de routage. À l'instar de l'organisation des opérateurs, tous les réseaux de même destination seront agrégés en une unique route dans les tables de routage. Ce type de structuration du plan d'adressage convient aux organisations qui sont chargées de l'infrastructure globale d'interconnexion, en général des opérateurs ou les entités chargées des réseaux d'interconnexion des grandes organisations.

Type d'usage d'abord

Si le type d'usage des réseaux est d'abord privilégié, l'optimisation des entrées dans les tables de routage n'est alors pas envisageable. Cependant, cela n'est en général pas un problème pour la plupart des routeurs modernes, qui peuvent gérer un nombre conséquent d'entrées de table de routage. L'avantage de grouper les réseaux par catégorie d'usage est que cela facilite l'application des politiques de sécurité. La plupart des équipements de sécurité (pare-feux, listes de contrôles d'accès, contrôle des autorisations…) sont régis selon les types d'usages plutôt que sur la localisation des utilisateurs. Les organisations choisissent communément de privilégier les types d'usages sur la localisation pour des raisons pratiques. L'application des politiques de contrôle d'accès et de sécurisation, basées sur des listes de filtres logiques, est généralement déléguée à des équipements spécialisés de type pare-feu, placés frontalement à l'entrée du réseau. Une fois contrôlés, les flux sont ensuite acheminés en interne en fonction de leur localisation.

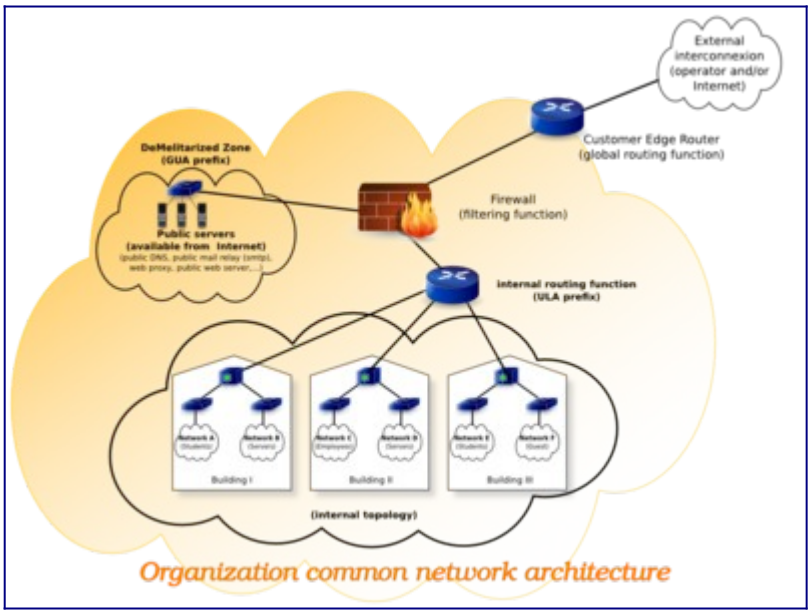

Figure 5 : Adressage structuré par localisation/usage.

Détermination de l'espace nécessaire au plan d'adressage

Nous devons déterminer quelle proportion des 16 bits du SID sera nécessaire pour chaque partie de cette structuration. Le nombres de bits nécessaires pour coder chacune des catégories de la structuration est conditionné par le nombre de types et de localisations de sous-réseaux de l'infrastructure, en ne négligeant pas les évolutions.

1. Déterminer le nombre de localisations ou types de réseaux de votre organisation ;
2. Augmenter le nombre d'une localisation supplémentaire, nécessaire pour le backbone ;
3. Augmenter le nombre de localisations pour tenir compte d'éventuels sous-réseaux qui n'ont pas de localisation fixe, tels que l'infrastructure des tunnels VPN par exemple ;
4. Augmenter le nombre de chacune des catégories pour tenir compte des expansions de court et moyen terme.

Pour chacune des catégories, déterminer la puissance de deux immédiatement supérieure ou égale, ce qui nous indiquera le nombre de bits nécessaires pour en coder les références.

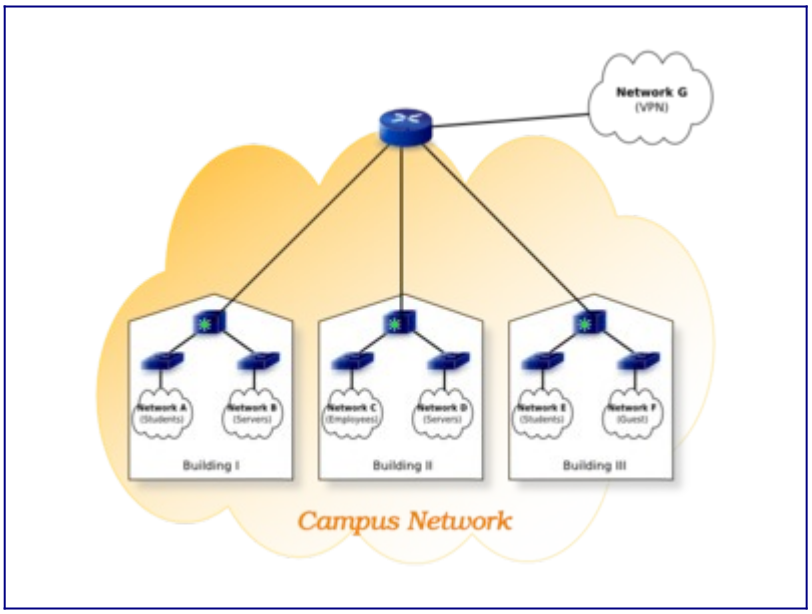

Figure 6 : Plan d'adressage structuré.

Exemple 1 : sous-réseaux basés sur la localisation

- nombre de localisations : 3
- backbone d'interconnexion (réseau reliant switchs et routeurs) : 1
- réseaux non localisés (tunnels VPN) : 1
- extension future : 2

total : 7 sous-réseaux => 3 bits suffisent pour encoder les localisations, le reste pouvant être utilisé pour d'autres référencements.

`2001:db8:cafe:{LLLBBBBBBBBBBBBB}::/64`

Exemple 2 : sous-réseaux basés sur le type d'usage

- nombre de groupes d'usage (personnel, étudiants, invités, serveurs, infra VPN) : 5 sous-réseaux,
- backbone et infrastructure (réseau reliant switchs et routeurs) : 1 sous-réseau,
- usages futurs : 4 sous-reseaux

total : 10 sous-réseaux => 4 bits suffisent pour encoder les types de sous-réseaux, les 12 bits restants pouvant être utilisés pour d'autres référencements.

`2001:db8:cafe:{TTTTBBBBBBBBBBBB}::/64`

Hiérarchisation à 2 niveaux

Dans les deux exemples précédents, les bits restants peuvent être utilisés pour numéroter un second niveau de sous-réseaux. Si la numérotation primaire est basée sur la localisation, plusieurs sous-réseaux peuvent être adressés sur chaque site. Si la numérotation primaire est par type d'usage, alors plusieurs réseaux de chaque type peuvent être créés (les réseaux internes réservés au personnel peuvent être déclinés par service ou fonction : comptabilité, RH,

direction, production...). Les deux types de structuration, localisation / type d'usage, peuvent également se combiner. Si on choisit de privilégier la location en structure primaire :

`2001:db8:cafe:{LLLTTTTBBBBBBBBB}::/64`,

il reste 9 bits pouvant coder 512 instances de sous-réseaux de chaque type sur chaque site. Le fait de privilégier la localisation, en positionnant sa référence sur les bits de poids fort du SID, facilitera l'optimisation des tables de routage de l'infrastructure d'interconnexion des sites. Cependant, elle alourdira les politiques de sécurisation en multipliant les filtres, si la fonction de sécurisation (firewall) est centralisée, ou elle imposera de disposer d'une fonction de sécurisation (firewall) sur chaque site, entraînant des difficultés de cohérence de déploiement des politiques de sécurité. Inversement, privilégier le type d'usage sur la localisation

`2001:db8:cafe:{TTTTLLLBBBBBBBBB}::/64`,

réduira le nombre de filtres de la politique de sécurisation au détriment du nombre d'entrées dans les tables de routage de l'interconnexion. Cependant, cela ne pose en général pas de difficultés majeures compte tenu des capacités des routeurs modernes.

Latitude

Dans l'exemple précédent, 4 bits sont utilisés pour les types de sous-réseaux et 3 pour la localisation, laissant 9 bits, soit 512 (2 puissance 9) sous-réseaux possibles par type et par site. Cela sera suffisant dans la plupart des cas. Cependant, imaginons qu'il faille 2048 tunnels VPN par site pour accueillir les connexions sécurisées des personnels nomades. On pourrait envisager de modifier les tailles de champs de structuration primaire et secondaire, mais cela nécessiterait une reconfiguration globale de l'architecture. Une autre option consiste à répartir les tunnels sur 4 types distincts, chacun pouvant gérer 512 tunnels. De cette manière, on conserve une politique de sécurité simple et cohérente.

Type	Usage
0	**Backbone, infrastructure**
1	**Serveurs**
2	Réservé expansion future
3	Réservé expansion future
4	**Personnels**
5	**Étudiants**
6	**Invités**
7	Réservé expansion

	future	
8	**VPN**	
9	**VPN**	
a	**VPN**	
b	**VPN**	
c	Réservé future	expansion
d	Réservé future	expansion
e	Réservé future	expansion
f	Réservé future	expansion

Lisibilité

Lorsque l'on dispose d'un espace d'identification suffisamment large, dans notre cas de champ SID sur 16 bits nous laissant 9 bits 'B' de marge, il est de bonne pratique d'aligner les identifiants sur des frontières de mots de 4 bits (quartet) pour faciliter la lisibilité des préfixes notés en hexadécimal. Ainsi, dans notre exemple, si on étend l'identifiant de la localisation sur 4 bits au lieu de 3, elle sera visuellement facilement identifiée par un opérateur humain lors de la lecture des adresses. Le format des adresses de nos exemples devient donc :

```
2001:db8:cafe:{LLLLTTTTBBBBBBBB}::/64
2001;db8:cafe:{TTTTLLLLBBBBBBBB:}:/64
```

soit, en notation canonique, des adresses respectivement

```
2001:db8:cafe:wxyz::/64
2001:db8:cafe:xwyz::/64
```

avec les "nibbles" **w** pour identifier la localisation et **x** pour le type de sous-réseau.

Extensibilité

Si le nombre de localisations ou de types de sous-réseaux n'est pas à priori connu au moment de l'établissement du plan d'adressage, il est recommandé de conserver des frontières flexibles entre les différents groupes de bits identifiants les différents niveaux de la structuration. Cela peut être réalisé en adoptant une des stratégies décrites dans les RFC 1219 et RFC 3531. La contrepartie de cette approche est q'une certaine aisance dans la manipulation des bits doive être acquise, dans la mesure ou les frontières des zones d'identification peuvent être amenées à évoluer, ce qui peut nécessiter des mises à jour des règles et filtres de la politique de sécurité. Ainsi, par exemple, en assumant une structuration où l'on privilégie d'abord la localisation des

sous-réseaux assignée aux bits de poids fort, sur le type assigné au bits intermédiaires, un plan d'adressage flexible initialement conçu pour 5 localisations, 3 types et 2 sous-réseaux par localisation/type :

```
2001:db8:cafe:{LLL*****TT*****B}::/64
```

pourrait évoluer selon le scénario hypothétique suivant, passant de 2 à 10 sous-réseaux nécessitant 4 bits B.

```
2001:db8:cafe:{LLL*****TT**BBBB}::/64
```

Après cela, le nombre de types d'usages pourrait passer à 5, nécessitant un troisième bit T.

```
2001:db8:cafe:{LLL****TTT**BBBB}::/64
```

Puis, suite à une expansion géographique, le nombre de sites passerait à 50, portant à 6 le nombres de bits L.

```
2001:db8:cafe:{LLLLLL*TTT**BBBB}::/64
```

Si ensuite le nombre de types d'usages passait à 13, on étendrait le champ type par un quatrième bit pris sur la droite où il reste plus de bits disponibles.

```
2001:db8:cafe:{LLLLLL*TTTT*BBBB}::/64
```

Nota 1 : *les champs dont l'agrandissement s'effectue par la droite ({L} et {T} dans notre exemple) encodent les nombres selon un ordonnancement inhabituel. Le RFC 3531 décrit précisément les référencements de croissance gauche (les bits {B} dans notre exemple), centrale (les bits {T} dans notre exemple), ou droite (les bits {L} dans notre exemple).*

Nota 2 : *cette stratégie prenant en compte les besoins d'extensibilité peut s'avérer difficilement conciliable avec l'objectif de lisibilité préconisant un alignement sur les quartets tel que décrit dans le paragraphe précédent.*

Identification des sous-réseaux d'après les VLAN

Confinement des domaines de diffusion de niveau 2 : les VLAN

Ethernet est le protocole dominant de niveau liaison de données (niveau 2 de la pile protocolaire), support du niveau réseau IPv6, des infrastructures de réseaux de la plupart des organisations. Les architectures Ethernet modernes, constituées de commutateurs (switchs Ethernet) sont généralement subdivisées en différents domaines de diffusion étanches, couramment dénommés VLAN. Cette structuration en VLAN permet de constituer des groupes logiques de machines partageant un même support de diffusion. Chaque VLAN Ethernet dispose d'un identifiant propre (VLAN-ID). Au niveau réseau (niveau 3 de la pile protocolaire), où opère le protocole IPv6, chaque VLAN se voit affecter un (ou plusieurs) identifiants de sous-réseaux distincts. En effet, deux postes localisés dans des VLAN distincts ne peuvent échanger directement des données et doivent passer une fonction de routage inter-réseaux (routeur) pour pouvoir communiquer.

Mise en correspondance VLAN-ID et SID

Une autre approche de structuration du plan d'adressage, sur ce type d'infrastructure, est de dériver l'identifiant de sous-réseau IPv6 (SID) de l'identifiant du domaine de diffusion (VLAN-ID). Les identifiants de VLAN Ethernet (VLAN-ID) qui ont une taille de 12 bits, 4094 VLAN distincts (les valeurs 0 et 4095 étant réservées), peuvent être créés sur une infrastructure locale. Dans notre cas de figure (préfixe en /48), où nous disposons de 16 bits pour identifier nos sous-réseaux IPv6, on peut envisager de faire coïncider VLAN-ID et SID soit sous leur forme hexadécimale, soit sous leur forme décimale.

- **Forme hexadécimale** : en convertissant la valeur décimale de l'identifiant de VLAN en hexadécimale pour le transposer en identifiant de sous-réseau sur trois quartets (nibble). Dans ce cas, il reste un quartet du champ SID libre, qui peut être utilisé pour éventuellement coder 16 localisations ou 16 types. Il faut alors décider de la position du quartet libre, soit sur le quartet de poids fort, soit sur le quartet de poids faible.

VLAN-ID sur les bits de poids fort du SID `2001:db8:cafe:{VVVVVVVVVVVVBBBB}::/64`

ou

VLAN-ID sur les bits de poids faible du SID `2001:db8:cafe:{BBBBVVVVVVVVVVVV}::/64`

Cependant, si les adresses IPv6 sont en notation hexadécimale (cf. activité 12), les identifiants de VLAN sont en notation décimale, ce qui ne facilite pas la lisibilité de correspondance lors de la lecture de l'adresse IPv6.

- **Forme décimale**. Afin de conserver une correspondance lisible entre l'identifiant de sous-réseau IPv6 et l'identifiant de VLAN, on peut conserver la valeur décimale du VLAN-ID et l'utiliser directement en lieu et place de l'identifiant SID hexadécimal. La correspondance est alors directement lisible. Ainsi, le sous-réseau IPv6 `2001:db8:cafe:4321::/64` sera affecté au VLAN 4321. On remarquera que les identifiants de sous-réseaux supérieurs à 4095 ainsi que ceux comportant une ou plusieurs lettres hexadécimales (a..f) sont disponibles pour d'autres sous-réseaux logiques non liés à un VLAN.

Tableau récapitulatif des deux approches.

VLAN-ID	IPv6 vlan-id forme décimale	IPv6 vlan-id forme hexadécimale poids faible	IPv6 vlan-id forme hexadécimale poids fort
1	2001:db8:cafe:000**1**::/64	2001:db8:cafe:0**001**::/64	2001:db8:cafe:**001**0::/64
12	2001:db8:cafe:00**1****2**::/64	2001:db8:cafe:0**00c**::/64	2001:db8:cafe:**00c**0::/64
2783	2001:db8:cafe:**278****3**::/64	2001:db8:cafe:0**adf**::/64	2001:db8:cafe:**adf**0::/64

4094	2001:db8:cafe:**409**4::/64	2001:db8:cafe:0**ffe**::/64	2001:db8:cafe:**ffe**0::/64

Cette approche introduit une certaine cohérence entre l'infrastructure de niveau 2 et l'adressage de niveau 3 et simplifie la numérotation des sous-réseaux IPv6 dans la mesure où une seule numération doit être gérée. Cependant, elle n'est pas optimale pour minimiser le nombre d'entrées dans les tables de routage ou pour optimiser les politiques de contrôle d'accès basées sur le filtrage des préfixes.

Identification des VLAN selon la localisation ou le type d'usage

Il est possible d'envisager un codage des VLAN-ID intégrant la localisation ou le type d'usage. Dans ce cas, il est souhaitable de conserver un alignement sur frontières de quartet (nibble). De ce fait, on peut choisir de coder la localisation sur 4 ou 8 bits {W} et coder respectivement le type sur 8 ou 4 bits {V} ou inversement. De même, comme pour la hiérarchisation à deux niveaux vue précédemment, il faudra choisir de privilégier soit la localisation soit le type en le positionnant sur les bits de poids fort.

- **Forme hexadécimale**. Dans cette forme, sur un SID long de 16 bits, on conserve 4 bits utilisables pour coder 16 instances de chaque localisation/type.

VLAN-ID sur les bits de poids fort du SID

localisation {W} sur 4 bits (1 quartet) privilégiée

`2001:db8:cafe:{WWWWVVVVVVVVBBBB}::/64`

ou

VLAN-ID sur les bits de poids fort du SID

localisation {W} sur 8 bits (2 quartets) privilégiée

`2001:db8:cafe:{WWWWWWWWVVVVBBBB}::/64`

Inversement, si on privilégie le type d'usage

VLAN-ID sur les bits de poids fort du SID

type d'usage {V} sur 4 bits (1 quartet) privilégié

`2001:db8:cafe:{VVVVWWWWWWWWBBBB}::/64`

ou

VLAN-ID sur les bits de poids fort du SID

type d'usage {V} sur 8 bits (2 quartets) privilégié

`2001:db8:cafe:{VVVVVVVVWWWWBBBB}::/64`

Quelques exemples illustratifs de la forme hexadécimale (localisation sur 1 quartet, type d'usage sur 2 quartets)

VLAN-ID		**localisation**		**Type d'usage**		**IPv6 (VLAN-ID hexadécimal)**
décimal	hexa	décimal	hexa	décimal	hexa	
0001	(001)	0	(**0**01)	1	(0**01**)	`2001:db8:cafe:001`**0**`::/64`
0529	(211)	2	(**2**11)	17	(2**11**)	`2001:db8:cafe:211`**0**`::/64`
4094	(ffe)	15	(**f**fe)	254	(f**fe**)	`2001:db8:cafe:ffe`**0**`::/64`

- **Forme décimale**. La lisibilité directe est alors conservée mais chaque quartet (nibble) ne peut prendre qu'une valeur numérique (0..9). Il ne reste plus de bits du SID disponibles pour coder d'éventuelles instances de chaque type/localisation. Cependant, on pourra choisir d'affecter un, deux ou trois quartets pour coder 10, 100, ou 1000 localisations, avec respectivement 1000, 100, 10 types d'usage.

`2001:db8:cafe:1025::/64`

VLAN 1025, localisation (1) type d'usage (025)

cas de la localisation sur 1 quartet et type d'usage sur 3 quartets

ou

VLAN 1025, localisation (10) type d'usage (25)

cas de la localisation sur 2 quartets et type d'usage sur 2 quartets

ou

VLAN 1025, localisation (102) type d'usage (5)

cas de la localisation sur 3 quartets et type d'usage sur 1 quartet

Quelques exemples illustratifs de la forme décimale (localisation sur 2 quartets, type d'usage sur 2 quartets).

VLAN-ID	**localisation**	**Type d'usage**	**IPv6(VLAN-ID forme décimale)**

0001	00	01	2001:db8:cafe:**0001**::/64
0529	05	29	2001:db8:cafe:**0529**::/64
4094	40	94	2001:db8:cafe:**4094**::/64

Conclusion

La représentation des adresses IPv6, les différents types et fonctions d'usage vous sont maintenant connus. Par la pratique et l'usage régulier, l'adressage IPv6 va naturellement et rapidement vous devenir familier. Vous pouvez cependant vous aider d'aide-mémoire de type tout en une page[1]. Si, comme nous l'évoquions au début de la séquence, le nouveau plan d'adressage nous met à l'abri de la pénurie, les avantages du nouveau protocole ne se résument pas à l'abondance des préfixes disponibles pour les nouveaux réseaux.

L'expérience acquise avec IPv4 a permis d'optimiser IPv6 dès sa conception. De nouvelles fonctionnalités telles que l'auto-configuration des paramètres ou la découverte de voisins, ont été intégrées dans le protocole. Ces fonctionnalités sont également des arguments en faveur de l'adoption d'un protocole moderne. C'est ce que vous allez découvrir dans les prochaines séquences.

Références bibliographiques

1. ↕ Carrell Jeffrey L. (2020) site Teach Me IPv6. IPv6 Essentials Referecence sheet